Manual - English

FUJITSU

FUJITSU Software ServerView Suite

ServerView Plug-in for VMware vCenter V2.1

April 2015

Comments… Suggestions… Corrections…

The User Documentation Department would like to know your opinion of this manual. Your feedback helps us optimize our documentation to suit your individual needs.

Feel free to send us your comments by e-mail to manuals@ts.fujitsu.com.

Certified documentation according to DIN EN ISO 9001:2008

To ensure a consistently high quality standard and user-friendliness, this documentation was created to meet the regulations of a quality management system which complies with the requirements of the standard DIN EN ISO 9001:2008.

cognitas. Gesellschaft für Technik-Dokumentation mbH
www.cognitas.de

Copyright and Trademarks

Copyright © 2015 Fujitsu Technology Solutions GmbH.

All rights reserved.
Delivery subject to availability; right of technical modifications reserved.

All hardware and software names used are trademarks of their respective manufacturers.

Contents

1 Overview 9

1.1 Integration approaches 11
1.2 Monitoring possibilities 11
1.3 Changes since the previous version 13
1.4 Target groups and purpose of this manual 14
1.5 Documentation for ServerView Suite 14
1.6 Abbreviations 14
1.7 Notational conventions 15

2 Installing on Windows 17

2.1 Provisioning 17
2.2 Prerequisites 17
2.3 Installation hints 18
2.4 Installing and registering 19
2.4.1 Installing procedure 20
2.4.2 Verifying the deployment 21
2.4.3 IPMI configuration 22
2.5 Updating 23
2.6 Unregistering and uninstalling 23
2.6.1 Unregistering the SV Plug-in package 23
2.6.2 Uninstalling the SV Plug-in 24

3 Installing on Linux 25

3.1 Provisioning 25
3.2 Prerequisites 25
3.3 Installation hints 26
3.4 Installing and registering 27
3.4.1 Installation parameters 27

3.4.2 Installing procedure 28
3.4.3 Installation examples 31
3.5 Updating 31
3.6 Unregistering and uninstalling 32

4 Log in to vCenter Server using the vSphere Web Client . . . 33

4.1 Prerequisites and localization 33
4.2 Procedure 33
4.3 vSphere Web Client user interface 34

5 Configuration tasks and concepts 37

5.1 SVvCenter Service configuration 37
5.1.1 Opening the SVvCenter Service Configuration Overview 37
5.1.2 Adding a vCenter to the SVvCenter Service 38
5.1.3 Updating the vCenter credentials 39
5.1.4 Removing a vCenter from the SVvCenter Service 40
5.2 IPMI configuration 40
5.3 FUJITSU PRIMERGY vCenter role definitions and iRMC single sign-on 42
5.3.1 FUJITSU PRIMERGY vCenter role definitions 42
5.3.2 Change privileges of a role definition 43
5.3.3 Starting iRMC functions with/without single sign-on 44
5.3.3.1 Prerequisites for single sign-on 44
5.3.3.2 iRMC functions with single sign-on 45
5.3.3.3 iRMC S4 Web Interface SSO enhancements 45
5.3.4 Examples of using role definitions to limit iRMC functionality . . . 49
5.3.4.1 vCenter user "monitor" and iRMC access without SSO (iRMC S2, S3, S4) 50
5.3.4.2 vCenter user "monitor" and iRMC access with SSO as iRMC user "user" 51
5.3.4.3 vCenter user "monitor2" and iRMC "user" access and extended privilege "RemoteStorage" 53

6 SV Plug-in Getting Started and Summary 57

6.1 Entry point 57

6.2 Tabs of the home page of the SV Plug-in 58

6.3 Tab Getting Started 58

6.4 Tab Summary 59

6.5 Tab Manage 61
6.5.1 Event Definitions 61
6.5.2 Alarm Definitions 62
6.5.3 Role Definitions 63

7 Monitoring ESXi-based hosts 65

7.1 Access to the SV Plug-in information of an ESXi-based host 65

7.2 SV Plug-in information of an ESXi-based host 67
7.2.1 Information on the selected host - Status items and views . . . 67
7.2.2 FUJITSU PRIMERGY Actions (iRMC-based operations) 71
7.2.2.1 Starting a FUJITSU PRIMERGY Action 72
7.2.2.2 The FUJITSU PRIMERGY Actions 73

7.3 Storage view 76

7.4 System Event Log view 78

8 Monitoring PRIMERGY blade servers 81

8.1 Access to the SV Plug-in information of an MMB 82

8.2 SV Plug-in information of an MMB node 83
8.2.1 Monitor tab: Information on the selected MMB - Status items and views 84
8.2.2 FUJITSU PRIMERGY Actions 86

8.3 SVvCenter Service for MMBs 87
8.3.1 Overview 87
8.3.2 SNMP settings 88
8.3.3 Receiving SNMP traps 89

9 Monitoring PRIMEQUEST systems 91

9.1 Access to the SV Plug-in information of a PRIMEQUEST system 92

9.2 SV Plug-in information of a PRIMEQUEST system 93
9.2.1 Monitor tab: Information on the selected PRIMEQUEST system - Status items and views 94
9.2.2 FUJITSU PRIMERGY Actions 97

9.3 SVvCenter Service for PRIMEQUEST systems 98
9.3.1 Overview 98
9.3.2 SNMP settings 99
9.3.3 Receiving SNMP traps 99

10 Monitoring vCenter or cluster host servers 101

10.1 Access to the SV Plug-in information of the hosts of a vCenter/cluster 101

10.2 FUJITSU PRIMERGY Actions 103

11 Integration in the event management of the vSphere Web Client 107

11.1 Prerequisites 109

11.2 SVvCenter Service Configuration Overview 110
11.2.1 Opening the SVvCenter Configuration Overview 110
11.2.2 Properties of SVvCenter Services 111
11.2.3 Further helpful service properties for the SVvCenter Service for Events, MMBs and PRIMEQUEST systems 112
11.2.4 Adding/removing a vCenter to/from the SVvCenter Service . . 113

11.3 FUJITSU PRIMERGY Predefined Alarm 113

11.4 Actions related to SVvCenter Service 114

12 Error handling 115

12.1 Point in time of data acquisition 115

12.2 All expanded items are closed 115

12.3 Retrieving data failed 115
12.4 An action at the top left of the SV Plug-in interface is disabled 115
12.5 An action in the context menu results an error message 116
12.6 Remote console (AVR) or iRMC Web Client don't work as was to be expected 116
12.7 The same event generates a significant number of entries in the event management 116
12.8 Repeated connection timeouts 117

1 Overview

Virtualization solutions from Fujitsu

Fujitsu is committed to total virtualization - from servers to storage to networks - and to virtualization software and operation management tools. The partnership between VMware and Fujitsu brings you continuity of technology assets, more efficient resource use, and steps toward the elimination of IT complexity.

VMware and Fujitsu ServerView integrated virtualization support

ServerView supports the CIM management standard, making it possible to monitor and manage VMware vSphere-based environments more reliably and securely. Administrators can view all physical and virtual machines through a single interface.

vSphere Web Client

VMware vSphere provides several interfaces for data center management and virtual machine access.

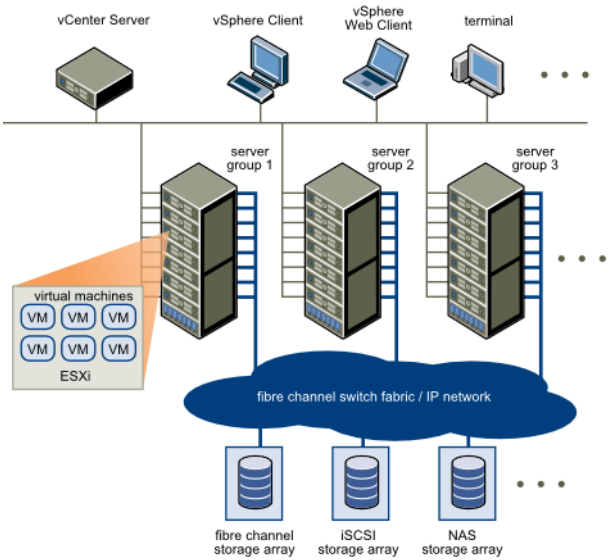


Figure 1: VMware vSphere data center physical topology - (Source: http://www.vmware.com/support/pubs/)

These interfaces include VMware vSphere Client (vSphere Client), vSphere Web Client for access through a Web browser, and vSphere Command Line Interface (vSphere CLI).

The vSphere Web Client is the primary method for system administrators and end users to interact with the virtual data center environment created by VMware vSphere. The vSphere Web Client is a Web browser-based application that you can use to manage, monitor, and administer the objects that make up your virtualized data center.

It is possible to extend vSphere in different ways to create a solution for a unique IT infrastructure. vSphere Web Client can be extended by creating plug-in modules. A complete plug-in solution adds new capabilities to the vSphere Web Client graphical user interface. In this way third-party companies can integrate their GUIs and show information as desired.

ServerView Suite and vSphere

The ServerView Suite has implemented the ServerView ESXi CIM Providers which are part of the VMware ESXi release. Additionally, Fujitsu has implemented the ServerView Plug-in for VMware vCenter (SV Plug-in) to the vSphere Web Client for vCenter which shows the values of a host system provided by the ServerView ESXi CIM providers and the LSI CIM providers (*Storage* view).

The ServerView Plug-in for VMware vCenter (SV Plug-in) offers you a home page with a *Getting Started* tab and a *Summary* tab, which gives an overview of the information items provided by the SV Plug-in.

The *Monitor* tabs for ESXi hosts, vCenters, Clusters, MMBs and PRIMEQUEST systems, the SV Plug-in provide you with detailed information about FUJITSU PRIMERGY servers. The information includes properties of the system, fans, temperature sensors, power supplies, system processors, memory modules, and of the RAID subsystem. In case the managed system is a PRIMERGY blade server there will be additional information about management-, server-, storage-, and connection-blades.

Additionally, the SV Plug-in includes the *SVvCenter Service* which routes FUJITSU PRIMERGY specific events to the vCenter event management to be monitored in the vSphere Web Client.

1.1 Integration approaches

The ServerView Plug-in for VMware vCenter (SV Plug-in) integrates FUJITSU PRIMERGY specific information in the vSphere Web Client interface. There are two approaches to do so:

Data integration
in event and alarm management of the vSphere Web Client itself

Full sites integrated
in the vSphere Web Client offer the FUJITSU PRIMERGY specific data of ESXi hosts, of hosts of vCenters or Clusters, of MMBs and of PRIMEQUEST systems

1.2 Monitoring possibilities

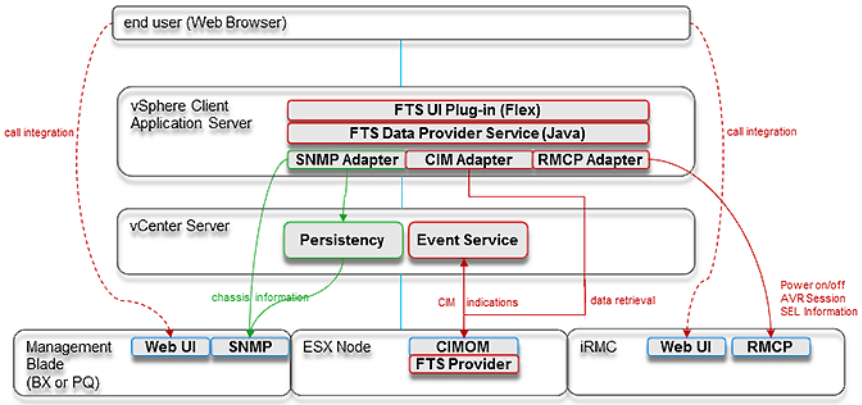


Figure 2: Architecture of the ServerView Plug-in for VMware vCenter

Extensive information on a selected host and FUJITSU PRIMERGY actions

The SV Plug-in offers extensive possibilities to monitor ESXi hosts, MMB blades or PRIMEQUEST systems: Status icons provide quick and detailed views provide extensive information on a selected host and a number of FUJITSU PRIMERGY actions items support calling a monitoring tool or doing settings on the host.

Monitoring vCenter or Cluster host servers

The SV Plug-in offers lists of the hosts assigned to a vCenter or to a Cluster. Via this access point the SV Plug-in offers less information on the single host than via the inventory tree item *Hosts*, but all FUJITSU PRIMERGY actions are available.

Monitoring PRIMERGY blade servers

To vSphere Web Client a MMB is a custom object type. To support custom object types, the object navigator vCenter level has to be extended with a new inventory list. The SV Plug-in adds the new inventory list *PRIMERGY Blade Server* to the object navigator vCenter level. The *SVvCenter Service* is used to make an discovery for all MMBs.

Monitoring PRIMEQUEST systems

To vSphere Web Client a PRIMEQUEST system is a custom object type. To support custom object types, the object navigator vCenter level has to be extended with a new inventory list. The SV Plug-in adds the new inventory list *PRIMEQUEST Server* to the object navigator vCenter level. The *SVvCenter Service* is used to make an discovery for all PRIMEQUEST systems.

SVvCenter Service - Integration in event and alarm management of vCenter

The SV Plug-in includes the *SVvCenter Service* which routes FUJITSU PRIMERGY specific events to the vCenter event management to be monitored in the vSphere Web Client. If a FUJITSU PRIMERGY host detects a problem, it will create a CIM indication and send it to subscribed destinations. Alarm is created too and can be configured for further actions. If SVvCenter Service is subscribed to the host, it will receive the CIM indication. It creates a vCenter event and forwards it to vCenter Server. So the FUJITSU PRIMERGY specific event is shown in the regular *Monitor-Events*-subtab of the vSphere Web Client.

System Event Log view and system indentification led

Events of PRIMERGY systems will be forwarded to the vSphere Event Manager. In addition, you can view the system event log including specialized cause and resolution information. To simplify service tasks the SV Plug-in provides the ability to turn the system indentification led of the PRIMERGY server on/off.

Remote Console (AVR) and iRMC Web interface - Configuration Web Application (MMB)

Furthermore, the SV Plug-in enables you to start a session with the onboard management controller (iRMC) of a managed PRIMERGY system via its web interface or to contact to a remote console. There are FUJITSU PRIMERGY vCenter role definitions designed for using single sign-on when starting the iRMC Web Interface and Remote Console.

In case the managed system is a PRIMERGY blade server you can start the Configuration Web Application of its management board (MMB) as well.

1.3 Changes since the previous version

This edition of the manual applies to ServerView Plug-in for VMware vCenter V2.1 and replaces the following online manual: "FUJITSU Software ServerView Suite, ServerView Plug-in for VMware vCenter V2.0", August 2014 edition.

The manual features the following changes and enhancements:

- Monitoring PRIMEQUEST systems, see "Monitoring PRIMEQUEST systems" on page 91.
- Four new role definitions have been added to the ServerView Plug-in for VMware vCenter. They are designed for using single sign-on when starting the iRMC Web Interface and Remote Console (AVR), see "FUJITSU PRIMERGY vCenter role definitions and iRMC single sign-on" on page 42 and "Role Definitions" on page 63.
- The installation packages (Windows/ Linux) include both, SV Plug-in and its SVvCenter Service.
- Remote installation possibility, see "Installation hints" on page 18 (Windows) and "Installation hints" on page 26 (Linux).
- Several vCenters - one installation: Once the SV Plug-in has been installed, you can connect annother vCenter to this vCenter Service, see "Installation hints" on page 18 (Windows) and "Installation hints" on page 26 (Linux).
- Extended event management:
  - A SVvCenter service routes PRIMEQUEST events to the vCenter event management to be monitored in the vSphere Web Client, see "Integration in the event management of the vSphere Web Client" on page 107.

  - The sub-tab *Event Definitions* of the *Manage* tab of the home page of the SV Plug-in lists the event definitions which are set by the SV Plug-in. The *Monitor Type* is added to the definition and the listing can be sorted according to its columns, see "Event Definitions" on page 61.

- The ServerView vCenter Service can be configured by some helpful settings, see "Further service properties" on page 112.

1.4 Target groups and purpose of this manual

This manual is intended for system administrators, network administrators and service technicians who already have a basic knowledge of hardware and software.

The manual explains how you can monitor a VMware vSphere-based server with ServerView and vSphere, and describes how to deploy the ServerView Plug-in for VMware vCenter.

1.5 Documentation for ServerView Suite

The documentation can be downloaded free of charge from the Internet. You will find the online documentation at *http://manuals.ts.fujitsu.com* under the link *x86 Servers*.

For an overview of the documentation to be found under *ServerView Suite* as well as the filing structure, see the ServerView Suite sitemap (*ServerView Suite - Site Overview*).

1.6 Abbreviations

SV Plug-in

In the following *SV Plug-in* is short for *ServerView Plug-in for VMware vCenter*.

1.7 Notational conventions

The following notational conventions are used in this manual:

Caution	This symbol points out hazards that can lead to personal injury, loss of data or damage to equipment.
	This symbol highlights important information and tips.
►	This symbol refers to a step that you must carry out in order to continue with the procedure.
italics	Commands, menu items, names of buttons, options, variables, file names and path names are shown in *italics* in descriptive text.
`fixed font`	System outputs are indicated using a `fixed font`.
`fixed font semi-bold`	Commands to be entered via the keyboard are written in a semi-bold fixed font.
<abc>	Angle brackets are used to enclose variables which are to be replaced by actual values.
Key symbols	Keys are shown according to their representation on the keyboard. If uppercase letters are to be entered explicitly, then the Shift key is shown, e.g. SHIFT - A for A. If two keys need to be pressed at the same time, this is indicated by hyphen between the two key symbols.

Table 1: Notational conventions

References to text or sections of text in this manual are shown with the chapter or section heading and the page on which that chapter or section begins.

Screen outputs

Please note that the screen output is dependent in part on the system used and therefore some details may not correspond exactly to the output you will see on your system. You may also see system-dependent differences in the menu items available.

2 Installing on Windows

The installation package includes both, SV Plug-in and its SVvCenter Service.

2.1 Provisioning

You can obtain the SV Plug-in in the following ways:

– Download from the Fujitsu website:

  ► Choose *Support* - *Computing products* - *Servers*.

  ► Click the link *Drivers & Downloads*.

  ► Enter in the field *Driver Quicksearch*: `vcenter plug-in`.

  The entry *FUJITSU Software ServerView Plug-in for VMware vCenter* is displayed in the field *Search result* on tab *Drivers & Downloads*.

– Download from the ServerView Suite DVD.

2.2 Prerequisites

– The vCenter/ vSphere version must be at least 5.5.

  vCenter/ vSphere must be installed

  on

  Windows 2008 R2 (x64)

  or

  on Windows Server 2012

  Support of Windows Server 2012 starts with vCenter/ vSphere version 5.5 Update 1.

  or

on Windows Server 2012 R2
(see *http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17*)

Microsoft Windows Server 2012 R2 starts with vSphere Client (Windows) - 5.5 U1

Microsoft Windows Server 2012 R2 starts with vCenter Server - 5.5 U1

– Java runtime V1.6 or higher.

– Verify that vCenter Server is installed and that both vCenter Server and vSphere Web Client point to the same vCenter single sign-on instance.

2.3 Installation hints

Installation hint: Remote installation

You can install the plug-in package on a different system than where vCenter resides.

Installation default for SV Plug-in is local installation on a vCenter system.

Installation hint: Several vCenters - one installation

Prerequisite:
The vCenter systems are within the same single sign-on environment.

Once the SV Plug-in has been installed, you can connect annother vCenter to this SVvCenter Service: If another vCenter system (vC2) is within the same single sign-on environment, it is possible to connect this vCenter (cV2) to the SVvCenter Service (Service1) of a vCenter (vC1).

In this case, after username and password have been entered, the vCenter (vC2) will be monitored by the SVvCenter Service (Service1) and the SV Plug-in will be registered on vCenter (vC2) as well. The SV Plug-in will be available for the hosts in vCenter (vC2), and you can monitor their values.

Because of the SV Plug-in will be registered on vCenter (vC2) as well, it is not necessary to perform a second installation. If you disconnect a vCenter, the SV Plug-in will be unregistered from that vCenter.

2.4 Installing and registering

A plug-in package contains all of the plug-in modules in an extension solution along with a package manifest. The package manifest describes deployment information for each plug-in module using XML metadata. The vSphere Web Client Extension Manager uses this metadata to install and deploy each plug-in module in the plug-in package.

You deploy a plug-in package to the vSphere Web Client by registering the package as an extension on vCenter Server. When you register your solution as an extension on vCenter Server, your solution becomes available to any vSphere Web Client that connects to your vSphere environment.

When a vSphere Web Client establishes a user session to vCenter Server, the vSphere Web Client application server queries vCenter Server for a list of all available plug-in packages that are registered as vCenter extensions. Any plug-in packages that are not present on the application server are downloaded and installed.

Localization:

Supported languages for installation on Windows are English and Japanese.

If the operating system language matches one of these languages, the corresponding language will be selected for installation of the SV Plug-in.

In case of other operating system languages English is default for installation of the SV Plug-in.

The SV Plug-in package:

The SV Plug-in package consists of the following files:

- sv_vcenter.exe
- sv_vcenter.ini
- sv_vcenter.msi
- sv_vcenter_ja.mst
- THIRDPARTYLICENSEREADME.txt

2.4.1 Installing procedure

- Execute the file *sv_vcenter.exe* on the vCenter Server server.

  A guided setup dialog is started.

- Provide necessary login information for vCenter.

  For registering the SV Plug-in with vCenter Server, the user name and password of a vCenter administration account are requested.

  Several vCenters - one installation (see "Installation hint: Several vCenters - one installation" on page 18):

  In this case, after username and password have been entered, the SV Plug-in will be registered on vCenter (vC2) as well. If you disconnect a vCenter, the SV Plug-in will be unregistered from that vCenter.

- Specify the settings for SVvCenter Service.

  If you install a SVvCenter Service on a vCenter Server system, you have to ensure that your entries *Name of the Plug-In service station* and *DNS suffix of the Plug-In service station* correspond to the *Server FQDN* entry in the dialog before.

  The setting *SNMP community strings(comma separated)* is used to discover blade servers, see "SNMP settings" on page 88.

  Only one EventService registration is allowed for a vCenter Server system. If a registration already exists for a vCenter Server system, you will be informed. If you are sure to want to overwrite this registration, you have to uninstall the corresponding SVvCenter Service.

  If the vCenter Server, on which the SV Plug-in is registered, is not reachable anymore, a dialog box with a force uninstall option will be displayed. If you choose forced uninstall the registration will not be removed.

Finished installation hints

To ensure consistency between vCenter Server extension registration and WebClient client plug-in administration you should restart all vSphere Web Client services which use the SV Plug-in.

It is recommended that both the java cache and browser cache be cleared after the installation of the SV Plug-in. This is especially important after an upgrade installation has been performed.

Be aware that after installation or update of the SV Plug-in the first login to vSphere Web Client can take significantly longer.

If another vCenter (vC2) is within the same single sign-on environment, it is possible to connect this vCenter (cV2) to the SVvCenter Service (Service1) of one vCenter (vC1) without a second installation (see "Installation hint: Several vCenters - one installation" on page 18).

2.4.2 Verifying the deployment

Use the *vCenter Managed Object Browser* to verify the deployment of the SV Plug-in.

The *vCenter Managed Object Browser* runs in a Web browser and is accessed by using the fully-qualified domain name or IP address for the vCenter Server system.

To access the *vCenter Managed Object Browser*

- Start a Web browser.
- Enter the fully-qualified domain name (or the IP address) for the vCenter Server system and add */mob*.

  For example: `https://<domain name or IPaddress>/mob`
- Enter the user account and password for the system.

  On first logon at the vSphere Web browser after install of the SV Plug-in the logon duration can be longer than at other times (can last up to several minutes).

  If warning messages regarding the SSL certificate appear, you can disregard them and continue to log in to the *vCenter Managed Object Browser*, if VMware is the certificate authority and you are not in a production environment.

  The *vCenter Managed Object Browser* is started.
- In the *vCenter Managed Object Browser* start window, click *content*.

  A window about the data object type *ServiceContent* opens.

- In the *ServiceContent* window, click *ExtensionManager*.

  The *ExtensionManager* window opens.

  In this window, the extension *com.fujitsu.primergy.ssv* is listed and you will find an entry: *com.fujitsu.primergy.eventservice*.

Additional check:

You will find a new SVvCenter Service dialog in the overview and administration pages of the SV Plug-in, see "Tab Summary" on page 59 and "SVvCenter Service configuration" on page 37.

2.4.3 IPMI configuration

Username and password for IPMI configuration must be configured in vCenter Server to perform certain operations:

ESXi host:

the iRMC-based operations: iRMC Web Interface together with single sign-on (SSO), AVR, location button LED and with ServerView ESXi CIM providers version less than 6.31 the System Event Log view (see "FUJITSU PRIMERGY Actions (iRMC-based operations)" on page 71)

The ServerView ESXi CIM providers version 6.31 or later support the System Event Log view. The entries will be retrieved over CIM automatically.

If the ServerView ESXi CIM providers version is less than 6.31, it will be necessary to configure the IPMI credentials (see "IPMI configuration" on page 40) to retrieve the System Event Log entries from the host.

- How to configure username and password for IPMI configuration see "IPMI configuration" on page 40.

2.5 Updating

Due to technical restrictions an upgrade installation is not supported for V2.1 of SV Plug-in.

Before installation of SV Plug-in V2.1 could be started, deinstallation of former version of SV Plug-in must be performed.

If you have changed the privileges in one of the FUJITSU PRIMERGY role definitions and you update the SV Plug-in version, the role definitions will be overwritten (see "Change privileges of a role definition" on page 43)!

2.6 Unregistering and uninstalling

2.6.1 Unregistering the SV Plug-in package

If you want to unregister and uninstall the SV Plug-in, see "Uninstalling the SV Plug-in" on page 24.

You can unregister the SV Plug-in package using the *vCenter Managed Object Browser* interface (see "Verifying the deployment" on page 21).

Several vCenters - one installation (see "Installation hint: Several vCenters - one installation" on page 18):

If you disconnect a vCenter, the SV Plug-in will be unregistered from that vCenter.

Unregistering a plug-in package on vCenter Server does not delete the plug-in package files that are installed locally on the *vSphere Web Client Virgo server*. The files are no longer used after the package has been unregistered, but if you want to remove them for cleanup purposes, you have to remove them manually. You can remove the files installed on the vCenter Server and unregister the SV Plug-in in one step by using the uninstall procedure (see "Uninstalling the SV Plug-in" on page 24).

2.6.2 Uninstalling the SV Plug-in

It is recommended only to use this option in case of failure of the vCenter Server system.

For uninstalling the SV Plug-in use the control panels option *Change*.

If the vCenter Server, on which the SV Plug-in is registered, is not reachable anymore, a dialog box with a force uninstall option will be displayed.

3 Installing on Linux

The installation package includes both, SV Plug-in and its SVvCenter Service.

3.1 Provisioning

You can obtain the SV Plug-in in different ways (see "Provisioning" on page 17).

Supported distributions:

– VMware appliances

– EVO:RAIL Management VM (CentOS 6.6 x86-64)

3.2 Prerequisites

The VMware vCenter Server Appliance (downloadable over VMware Download Center) is a preconfigured Linux-based virtual machine that is optimized for running vCenter Server and associated services (e.g. vSphere Web Client and SSO server).

– The vCenter/ vSphere version of the VMware vCenter Server Appliance must be at least 5.5.

– Before starting the Linux setup of the SV Plug-in, the VMware vCenter Server Appliance has to be configured as described in its startup screen.

– The VMware vCenter Server Appliance Certificate regeneration should be enabled. This could be done in the VMware vCenter Server Appliance's Administration GUI.

– It has to be verified:

  ► Verify that vCenter Server of the VMware vCenter Server Appliance is configured and running.

  ► Verify also that both vCenter Server and vSphere Web Client point to the same vCenter single sign-on instance.

3.3 Installation hints

Installation hint: Remote installation

Prerequisites:

- Java must be installed on the system where the SV Plug-in is installed.
- SVvCenter Service must be able to resolve the host name of the vCenter Server Appliance.

You can install the plug-in package on a different system than where vCenter resides (see "Installing and registering" on page 27).

Installation default for SV Plug-in is local installation on a vCenter system.

Installation hint: Scripted installation

Silent scripted installation is supported (see "Installing and registering" on page 27).

Installation hint: Several vCenters - one installation

Prerequisite:

The vCenter systems are within the same single sign-on environment.

Once the SV Plug-in has been installed, you can connect annother vCenter to this SVvCenter Service: If another vCenter system (vC2) is within the same single sign-on environment, it is possible to connect this vCenter (vC2) to the SVvCenter Service (Service1) of a vCenter (vC1).

In this case, after username and password have been entered, the vCenter (vC2) will be monitored by the SVvCenter Service (Service1) and the SV Plug-in will be registered on vCenter (vC2) as well. The SV Plug-in will be available for the hosts in vCenter (vC2), and you can monitor their values.

Because of the SV Plug-in will be registered on vCenter (vC2) as well, it is not necessary to perform a second installation. If you disconnect a vCenter, the SV Plug-in will be unregistered from that vCenter.

3.4 Installing and registering

A plug-in package contains all of the plug-in modules in an extension solution along with a package manifest. The package manifest describes deployment information for each plug-in module using XML metadata. The vSphere Web Client Extension Manager uses this metadata to install and deploy each plug-in module in the plug-in package.

You deploy a plug-in package to the vSphere Web Client by registering the package as an extension on vCenter Server. When you register your solution as an extension on vCenter Server, your solution becomes available to any vSphere Web Client that connects to your vSphere environment.

When a vSphere Web Client establishes a user session to vCenter Server, the vSphere Web Client application server queries vCenter Server for a list of all available plug-in packages that are registered as vCenter extensions. Any plug-in packages that are not present on the application server are downloaded and installed.

Localization:

Supported language for Linux package installation is English.

3.4.1 Installation parameters

For installation purposes there are the following parameters:

`-remote`
: Installation is done on a different system than where the vCenter resides (see "Installation hint: Remote installation" on page 26):

  Remote system: vCenter

  Local system: system the SV Plug-in is installed on

`-s | --silent`
: Possibility to run installation scripted

`-iplocal`
: IP address of system where installation is done

`-hostlocal`
: Host name of system where installation is done

`-dnslocal`
DNS-suffix of system where installation is done

`-ippreferred`
Using the given vCenter IP address as vCenter FQDN instead of using vCenter host name and vCenter DNS suffix

`-ipvcenter | -ip`
IP address of system where vCenter resides

`-hostvcenter | -host`
Host name of system where vCenter resides

`-dnsvcenter | -dns`
DNS-suffix of system where vCenter resides

`-pwvcenter | -pw | --password`
vCenter password

`-uservcenter | -u | --user`
vCenter user

3.4.2 Installing procedure

The Linux package will be delivered as a compressed *tar* archive (*ServerView*.tar.gz*).

Before installing the archive has to be transferred to the Linux-based virtual machine of the vCenter Server Appliance and has to be unpacked there (*tar -xvfz ...*).

To run the installation you have to perform the following steps:

- Copy the compressed *tar* archive to VMware vCenter Server Appliance.
- Extract the compressed *tar* archive.
- Change to the created subfolder.
- Start the installation with a */sv_install.sh* sequence.

  For examples of starting sequences according to different intentions see "Installation examples" on page 31.

  For command line options see "Installation parameters" on page 27. They will be displayed, if *sv_install.sh* is started with *-?* or *–help*.

  License Agreement is displayed before install or update of the SV Plug-in.

- The License Agreement has to be accepted.
- After the installation the SV Plug-in will be registered.

  For registering the SV Plug-in with vCenter Server, the user name and password of a vCenter administration account are requested.

  Several vCenters - one installation (see "Installation hint: Several vCenters - one installation" on page 26):

  In this case, after username and password have been entered, the SV Plug-in will be registered on vCenter (vC2) as well. If you disconnect a vCenter, the SV Plug-in will be unregistered from that vCenter.

- A check for an existing EventService registration is done.

  Only one EventService registration is allowed for a vCenter Server system. If a registration already exists for a vCenter Server system, you will be informed. If you are sure to want to overwrite this registration, you have to uninstall the corresponding SvvCenter Service.

Finished installation hints

To ensure consistency between vCenter Server extension registration and WebClient client plug-in administration you should restart all vSphere Web Client services which use the SV Plug-in.

It is recommended that the browser cache be cleared after the installation of the SV Plug-in. This is especially important after an upgrade installation has been performed.

Be aware that after installation or update of the SV Plug-in the first login to vSphere Web Client can take significantly longer.

If another vCenter (vC2) is within the same single sign-on environment, it is possible to connect this vCenter (cV2) to the SVvCenter Service (Service1) of one vCenter (vC1) without a second installation (see "Installation hint: Several vCenters - one installation" on page 26).

Verifying the deployment

- Use the *vCenter Managed Object Browser* to verify the deployment of the SV Plug-in (see "Verifying the deployment" on page 21).

IPMI configuration

Username and password for IPMI configuration must be configured in vCenter Server to perform certain operations:

ESXi host:

the iRMC-based operations: iRMC Web Interface together with single sign-on (SSO), AVR, location button LED and with ServerView ESXi CIM providers version less than 6.31 the System Event Log view (see "FUJITSU PRIMERGY Actions (iRMC-based operations)" on page 71)

The ServerView ESXi CIM providers version 6.31 or later support the System Event Log view. The entries will be retrieved over CIM automatically.

If the ServerView ESXi CIM providers version is less than 6.31, it will be necessary to configure the IPMI credentials (see "IPMI configuration" on page 40) to retrieve the System Event Log entries from the host.

- How to configure username and password for IPMI configuration see "IPMI configuration" on page 40.

3.4.3 Installation examples

According to different intentions there are examples of starting sequences:

Installation on a vCenter appliance:

```
sh sv_install.sh -iplocal 172.xx.xx.123 -ipvcenter
172.xx.xx.123 -hostvcenter vca550 -dnsvcenter
xxxx.xx.xx.net
```

Installation on a remote system:

```
sh sv_install.sh -iplocal 172.xx.xx.123 -ipvcenter
172.xx.xx.124 -hostvcenter vca550 -dnsvcenter
xxxx.xx.xx.net -remote
```

Installation on a remote system (scripted / EVO:RAIL):

```
sh sv_install.sh -iplocal 172.xx.xx.123 -ipvcenter
172.xx.xx.124 -hostvcenter vca550 -uservcenter vCuser
-pwvcenter vCpassword --silent
```

3.5 Updating

Due to technical restrictions an upgrade installation is not supported for V2.1 of SV Plug-in.

Before installation of SV Plug-in V2.1 could be started, deinstallation of former version of SV Plug-in must be performed.

If you have changed the privileges in one of the FUJITSU PRIMERGY role definitions and you update the SV Plug-in version, the role definitions will be overwritten (see "Change privileges of a role definition" on page 43)!

3.6 Unregistering and uninstalling

The SV Plug-in will be unregistered ...

The SV Plug-in will be unregistered in the uninstalling process before the RPM uninstallation is performed.

Several vCenters - one installation (see "Installation hint: Several vCenters - one installation" on page 26):

If you disconnect a vCenter, the SV Plug-in will be unregistered from that vCenter.

Uninstalling the SV Plug-in and/or the SVvCenter Service

To uninstall the SV Plug-in you have to perform the following steps:

- Initiate the uninstallation of the SV Plug-in by calling a *sv_install.sh* sequence with parameter *–e*.

  For examples of starting sequences according to different intentions see "Installation examples" on page 31.

  For command line options see "Installation parameters" on page 27. They will be displayed, if *sv_install.sh* is started with *-?* or *–help*.

  Before the RPM uninstallation is performed, a SVvCenter Service *clean* is executed which will unregister the SV Plug-in.

- The uninstallation will ask for the username and password of a vCenter administration account again.

  If the given passwords did not match, it is requested again.

  Otherwise the uninstallation continues.

4 Log in to vCenter Server using the vSphere Web Client

4.1 Prerequisites and localization

Prerequisites:

Verify that vCenter Server is installed and that both vCenter Server and vSphere Web Client point to the same vCenter single sign-on instance.

Localization:

Supported languages for using the SV Plug-in are English, German, and Japanese.

If the browser language matches one of these languages, the corresponding language will be selected for the SV Plug-in.

4.2 Procedure

- Open a Web browser and enter the URL for the vSphere Web Client: *https://client-hostname:port/vsphere-client*

  By default the port is 9443, but this can be changed during vSphere Web Client installation.
- In the *Username* text box, enter the user name that is registered on the vCenter single sign-on and has permissions on vCenter Server.
- In the *Password* text box, enter the password.
- Click *Login*.

  The vSphere Web Client connects to all the vCenter Server systems that the specified user has permissions for allowing you to view and manage your inventory.

4.3 vSphere Web Client user interface

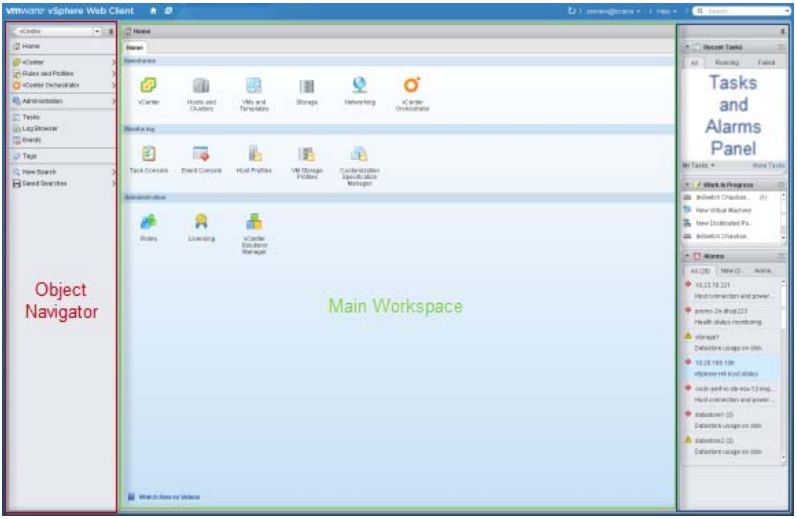


Figure 3: Major parts of the vSphere Web Client user interface (Source: www.vmware.com)

The user interface layer of the vSphere Web Client contains all of the Flex objects, such as data views, toolbars, and navigation interfaces, that make up the vSphere Web Client graphical user interface.

The major parts of the vSphere Web Client user interface are the *object navigator*, the *main workspace*, and the tasks and alarms panel. The user's selections in the object navigator drive the content of the vSphere Web Client main workspace.

In the object navigator *vCenter* level, vSphere objects are organized into *inventory trees* and *inventory lists*. When the user selects an object in the object navigator, information about that object appears in the main workspace.

When the user browses the virtual infrastructure using the object navigator, the main workspace displays an object workspace. Any given vSphere object has associated *Getting Started*, *Summary*, *Monitor*, *Manage*, and *Related Objects* top-level tab screens. Some of the se tabs contain second-level tabs and views within the tabs:

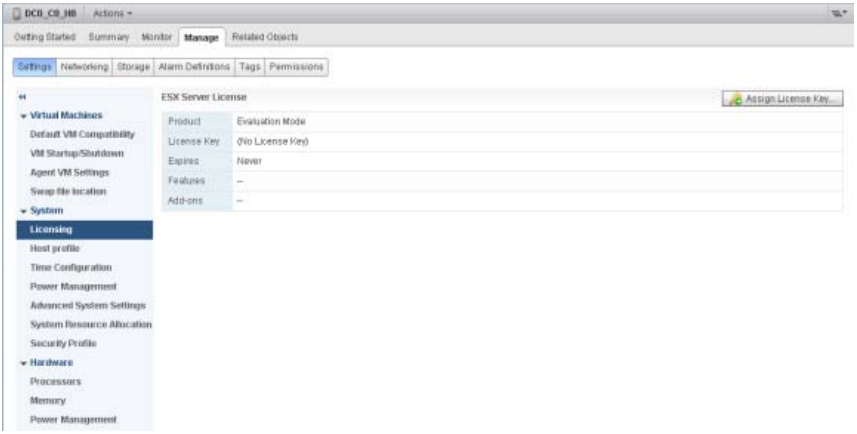


Figure 4: vSphere Web Client user interface: object workspace and its tabs (Source: www.vmware.com)

5 Configuration tasks and concepts

5.1 SVvCenter Service configuration

You can use the *SVvCenter Service Configuration Overview* to manage all of the SVvCenter Services installed in your environment.

Recommendation for performance reasons:

one SVvCenter Service for one vCenter server.

5.1.1 Opening the SVvCenter Service Configuration Overview

At the bottom of the getting-started tab of the home page of the SV Plug-in you find a link *Manage the SVvCenter Services*.

- In the object navigator of the vSphere Web Client select the item *Administration*.
- Select the sub-item *FUJITSU PRIMERGY Administration*.
- Select the sub-item *SVvCenter Service Configuration Overview*.

  In the main workspace of the vSphere Web Client the *SVvCenter Service Configuration Overview* opens:

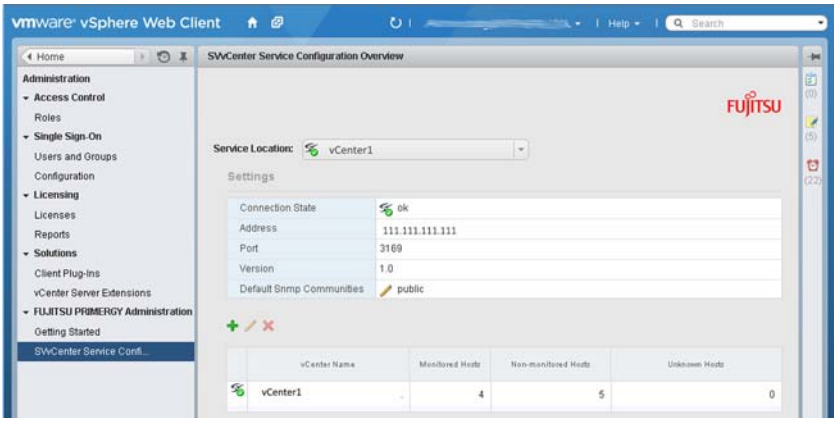


Figure 5: SVvCenter Service Configuration Overview

The setting *Default Snmp Communities* is used to discover blade servers (see "SNMP settings" on page 88). You can edit this list (comma separated) by clicking the pen-icon seen in this area.

SVvCenter Service has to be configured as a trap destination on the registered MMBs.

For further information see "Properties of SVvCenter Services" on page 111.

5.1.2 Adding a vCenter to the SVvCenter Service

The following procedure will help if a connection problem with a SVvCenter Service occurs:

If a vCenter is connected to a failing SVvCenter Service and you connect this vCenter to another SVvCenter Service, the vCenter will be disconnected from the failing SVvCenter Service and added to the selected new SVvCenter Service.

If you have changed the privileges in one of the FUJITSU PRIMERGY role definitions and you connect the vCenter (the role is assigned to) to another SVvCenter Service, the role definitions will be overwritten (see "Change privileges of a role definition" on page 43)!

- On the *SVvCenter Service Configuration Overview* select one SVvCenter Service in the *Service Location* selection box.

  The current properties of the selected SVvCenter Service are displayed.

► Click the + icon.

A dialog starts:

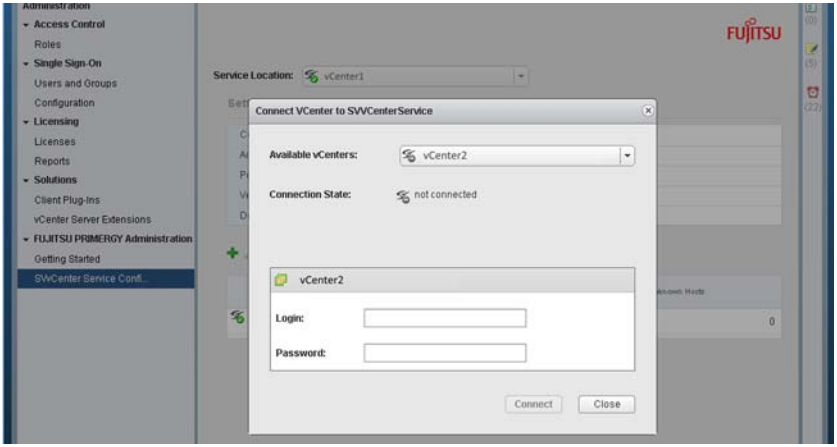


Figure 6: Add a vCenter to the SVvCenter Service

► Select one vCenter in the *Available vCenters* selection box.

The current connection status of the selected vCenter is displayed.

► Enter user name and password of the administrator account of the vCenter.

► Click *Connect*.

The vCenter is added to the SVvCenter Service.

The SVvCenter Service performs a discovery action for blade servers or PRIMEQUEST systems , subscribe itself to the hosts found in the vCenter, and forward any indications or traps to the vCenter.

5.1.3 Updating the vCenter credentials

It may be necessary to update the credentials of a vCenter, i.e. if the administrator password has changed.

► On the *SVvCenter Service Configuration Overview* select one SVvCenter Service in the *Service Location* selection box.

The current properties of the selected SVvCenter Service are displayed.

► In the *vCenter Name* list select the desired vCenter.

- ► Click the pen-icon.

  A dialog starts.
- ► Enter user name and password of the administrator account of the vCenter.
- ► Click *Update Connection*.

  The vCenter credentials are updated on the SVvCenter Service.

5.1.4 Removing a vCenter from the SVvCenter Service

> **i** A SVvCenter Service requires at least one vCenter to be connected. Therefore, it is only possible to disconnect a vCenter if more than one vCenter is connected. To disconnect all vCenters from a SVvCenter Service uninstall the SVvCenter Service.

- ► On the *SVvCenter Service Configuration Overview* select one SVvCenter Service in the *Service Location* selection box.

  The current properties of the selected SVvCenter Service are displayed.
- ► In the *vCenter Name* list select the desired vCenter.
- ► Click the *X* icon.

  The vCenter is disconnected from the SVvCenter Service.

5.2 IPMI configuration

Username and password for IPMI configuration must be configured in vCenter Server to perform certain operations:

> **i** Be careful when editing the credential information. When invalid credentials are entered, it may take a few minutes before you see an error message. If the IPMI is configured, and wrong credentials are entered, no change in the configuration will take place.

ESXi host:

the iRMC-based operations: iRMC Web Interface together with single sign-on (SSO), AVR, location button LED and with ServerView ESXi CIM providers version less than 6.31 the System Event Log view (see "FUJITSU PRIMERGY Actions (iRMC-based operations)" on page 71)

The ServerView ESXi CIM providers version 6.31 or later support the System Event Log view. The entries will be retrieved over CIM automatically.

If the ServerView ESXi CIM providers version is less than 6.31, it will be necessary to configure the IPMI credentials (see "IPMI configuration" on page 40) to retrieve the System Event Log entries from the host.

Procedure:

The iRMC user account must have the LAN channel privilege of *administrator* or *oem* to use single sign-on when starting iRMC, or to start other IPMI actions from the SV Plug-in. It is possible however, to limit the iRMC privileges depending on the role of the current vCenter user. For further information see "Starting iRMC functions with/without single sign-on" on page 44.

- Log in to vCenter Server using the vSphere Web Client (see "Log in to vCenter Server using the vSphere Web Client" on page 33).
- Start the *FUJITSU PRIMERGY Action Configure IPMI* (see for an ESXi host: "Starting a FUJITSU PRIMERGY Action" on page 72).
- Click the item/ the icon *IPMI Configuration*.

  The following dialog is displayed:

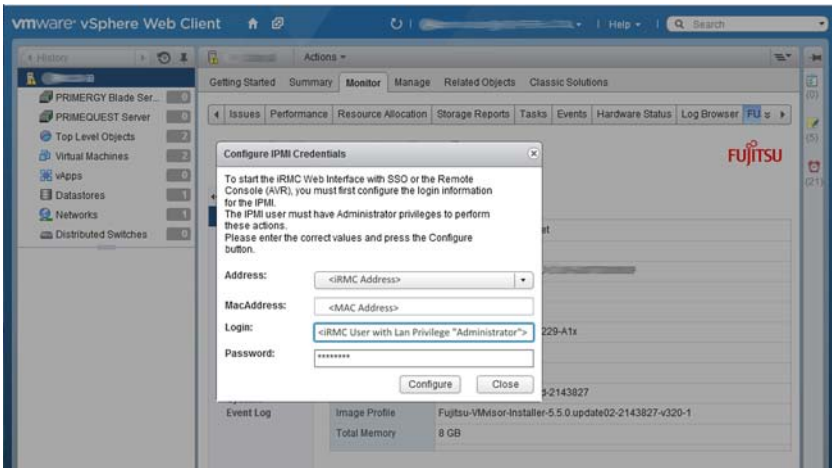


Figure 7: IPMI configuration dialog of the SV Plug-in (example: for an ESXi host)

- Enter *Login* and *Password*.
- Click *Configure* to send and store the user credentials in vCenter Server.

Once this user credentials information is stored in vCenter Server you only have to do this in cause of changes (for example: the credentials have been changed on the host).

5.3 FUJITSU PRIMERGY vCenter role definitions and iRMC single sign-on

Four new role definitions have been added to the SV Plug-in. They are designed for using single sign-on when starting the iRMC Web Interface and Remote Console (AVR). All role definitions contain the system privileges as well as the privilege *Host.CIM.Interaction* because that is needed to operate the SV Plug-in itself. For further information see "FUJITSU PRIMERGY vCenter role definitions" on page 42.

It is possible to add the extended iRMC privileges to a FUJITSU PRIMERGY vCenter role definition, see "Starting iRMC functions with/without single sign-on" on page 44. Additional, you can use the FUJITSU PRIMERGY vCenter role definitions to limit iRMC functionality, see "Examples of using role definitions to limit iRMC functionality" on page 49.

The sub-tab *Role Definitions* of the *Manage* tab of the home page of the SV Plug-in (see "Role Definitions" on page 63) lists the predefined FUJITSU PRIMERGY roles. If the role definitions have been reconfigured after installation, the changes relevant to proper processing of the SV Plug-in will be marked.

5.3.1 FUJITSU PRIMERGY vCenter role definitions

Four new role definitions have been added to the SV Plug-in:

FUJITSU PRIMERGY Plug-in Administrator
: Contains all the privileges needed to start the iRMC Web Interface and AVR using single sign-on with the iRMC LAN channel privilege level of *Administrator*.

  The user can also change the configuration for alarms.

FUJITSU PRIMERGY Plug-in Super Operator

Contains a subset of the SV Plug-in *Administrator* privileges which are needed to start the iRMC Web Interface using single sign-on with the iRMC LAN channel privilege of *Operator*, plus the extended iRMC privileges *ConfigureBMC*, *RemoteStorage* and *AVR*.

The user can make some configuration changes (but for example no firmware changes).

The user can also acknowledge alarms.

The user can start AVR from within the iRMC Web Interface.

FUJITSU PRIMERGY Plug-in Operator

Contains only the privileges need to start the iRMC Web Interface using single sign-on with the iRMC LAN channel privilege of *Operator*, plus the extended iRMC privilege *AVR*.

The user will be able to perform shutdown/reboot on the host, but cannot make any configuration changes.

The user can also acknowledge alarms.

The user can start AVR from within the iRMC Web Interface.

FUJITSU PRIMERGY Plug-in Monitor

Contains only the privileges need to start the iRMC Web Interface using single sign-on with the iRMC LAN channel privilege of *User*, plus the extended iRMC privilege *AVR*.

The user can start AVR from within the iRMC Web Interface.

5.3.2 Change privileges of a role definition

The sub-tab *Role Definitions* of the *Manage* tab of the home page of the SV Plug-in lists the predefined FUJITSU PRIMERGY role definitions, which are generated during the installation process (see "Role Definitions" on page 63).

If the role definitions have been reconfigured after installation, the changes relevant to proper processing of the SV Plug-in will be marked.

Configuring the FUJITSU PRIMERGY role definitions

To change the privileges in one of these role defintions use the vSphere Web Client UI.

If you need to change the privileges in one of the FUJITSU PRIMERGY role definitions, clone the role and change the privileges in the clone.

If you update the SV Plug-in version, or connect the vCenter to another SVvCenter Service, the role definitions will be overwritten!

- In the object navigator of the vSphere Web Client select the item *Administration*.
- Select the sub-item *Roles*.
- Select a vCenter server system from the drop-down menu.
- Select a role and click *Edit role action*.
- Select privileges for the role.
- Click *OK*.

5.3.3 Starting iRMC functions with/without single sign-on

Single sign-on can be used when starting the iRMC functions as *Administrator*. If the host has an iRMC S4 firmware version which is at least 7.73F, the SSO environment is enhanced to allow single sign-on for less privileged users. When starting the iRMC Web Interface, their iRMC LAN channel privilege will be adjusted to match the privilege level of the vCenter user.

5.3.3.1 Prerequisites for single sign-on

To perform the iRMC functions with single sign-on, the following prerequisites must be met:

– The IPMI credentials must be configured with an iRMC user account which has *Administrator* / *OEM* LAN channel privilege (see "IPMI configuration" on page 40).

– The vCenter user must have the privileges defined in the FUJITSU PRIMERGY role definitions. The SV Plug-in role *Administrator* can perform single sign-on, lesser privileged users will be able to use single sign-on only with an iRMC S4 whose firmware version is at least 7.73F.

5.3.3.2 iRMC functions with single sign-on

Location button LED

If the IPMI credentials have been configured (see "IPMI configuration" on page 40), any vCenter user can toggle on/off the location button LED.

Remote console (AVR)

To directly start AVR with single sign-on, the vCenter user must have the privileges defined in the *FUJITSU PRIMERGY Plug-in Administrator* role (see "FUJITSU PRIMERGY vCenter role definitions" on page 42), however AVR can be started by any user from within the iRMC Web Interface.

iRMC Web Interface

If the vCenter user has the privileges defined in the *FUJITSU PRIMERGY Plug-in Administrator* role (see "FUJITSU PRIMERGY vCenter role definitions" on page 42), he will be able to start iRMC with single sign-on.

For all other cases, iRMC can be started with a login for the iRMC user.

5.3.3.3 iRMC S4 Web Interface SSO enhancements

If a host has an iRMC S4 with firmware version at least 7.73F, single sign-on access will be extended to the vCenter users with the *Super Operator, Operator* and *Monitor* roles.

It is possible to start the iRMC S4 Web Interface with one of three iRMC roles:

– administrator
– operator
– user

iRMC extended privileges

iRMC also offers four extended privileges which can be granted together with the roles:

- ConfigureBMC - perform system configuration on the host
- AVR - start AVR (Advanced Video Redirection)
- ConfigureUsers - configure user accounts (iRMC, CAS, LDAP)
- RemoteStorage - perform remote image and media operations

It is possible to use these extended privileges together with the iRMC roles. The ability to start AVR from within the iRMC Web Interface is granted to all users. Since the *ConfigureBMC* privileges allow extensive access to iRMC configuration functionality, it is recommended to use the predefined SV Plug-in *Super Operator* role (see "FUJITSU PRIMERGY vCenter role definitions" on page 42).

The *RemoteStorage* and *ConfigureUsers* privileges map to only a single vCenter privilege:

- RemoteStorage : Host.Config.Storage
- ConfigureUsers : Host.Local.ManageUserGroups

So they can be easily added to a SV Plug-in *Operator* or *Monitor* role (see "Examples of using role definitions to limit iRMC functionality" on page 49).

Correlation between the FUJITSU PRIMERGY SV Plug-in roles and iRMC S4 Web Interface functionality

The following table describes the correlation between the FUJITSU PRIMERGY SV Plug-in role definitions and iRMC S4 Web Interface functionality:

Predefined FUJITSU PRIMERGY vCenter role definition	iRMC LAN channel privilege	iRMC Web Interface functionality
FUJITSU PRIMERGY Plug-in Administrator	administrator	Can perform all functions provided in the iRMC Web Interface – View settings and information – Toggle on/off location button LED – Perform system shutdown/reboot – Remote image mount – Configure media options – Configure system settings – Raid configuration – Prime Collect – AIS Connect – System report – BIOS backup and update – iRMC reboot and update – Internal event log view/clear – Configure users – Start AVR

Predefined FUJITSU PRIMERGY vCenter role definition	iRMC LAN channel privilege	iRMC Web Interface functionality
FUJITSU PRIMERGY Plug-in Super Operator	operator + ConfigureBMC RemoteStorage AVR	– View settings and information – Toggle on/off location button LED – Perform system shutdown/reboot – Remote image mount – Configure media options – Configure system settings – Start AVR
FUJITSU PRIMERGY Plug-in Operator	operator + RemoteStorage AVR	– View settings and information – Toggle on/off location button LED – Perform system shutdown/rebooot – Remote image mount – Configure media options – Start AVR
FUJITSU PRIMERGY Plug-in Monitor	user + AVR	– View limited set of settings and information – Toggle on/off location button LED – Start AVR

5.3.4 Examples of using role definitions to limit iRMC functionality

This is an example to give a FUJITSU PRIMERGY SV Plug-in user *Monitor* limited access to the iRMC with single sign-on.

The administrator might wish to create a user with very limited privileges. He should be able to start the iRMC Web Interface with the LAN channel privilege of *user* and not make any changes on the system nor perform a system shutdown.

- A user is created (for example *monitor*).
- The target (vCenter, cluster or single host) is configured to have the permission:

  user: : monitor

  role: : *FUJITSU PRIMERGY Plug-in Monitor*

5.3.4.1 vCenter user "monitor" and iRMC access without SSO (iRMC S2, S3, S4)

Situation:

– When the user logs in, he can start iRMC Web Interface, but must log in using an iRMC user and password.

– He will have the LAN channel privileges corresponding to that account.

– The IPMI credentials will not be used.

vSphere Web Client:

User without SSO privileges (and iRMC firmware version lower than with 7.73F) or no IPMI credentials configured.

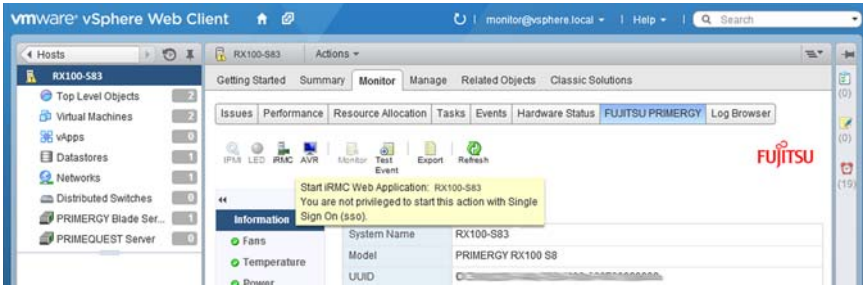


Figure 8: Example: vCenter user "monitor" and iRMC access without SSO - vSphere Web Client

SV Plug-in:

Figure 9: Example: vCenter user "monitor" and iRMC access without SSO - SV Plug-in

5.3.4.2 vCenter user "monitor" and iRMC access with SSO as iRMC user "user"

Situation:

– To provide SSO access for a *Super Operator*, *Operator* or *Monitor* vCenter user, a host must have an iRMC S4 with firmware version at least 7.73F.

– The IPMI credentials must be configured with an iRMC user who has LAN channel privilege of *Administrator* / *OEM* (see "Starting iRMC functions with/without single sign-on" on page 44) - for example: *admin* / *admin*.

When the user logs in, he will be able to start the iRMC Web Interface with SSO but only has the LAN channel privileges of *user*.

vSphere Web Client:

The figure 10 displays the view for a vCenter user with *FUJITSU PRIMERGY Plug-in Monitor* role, IPMI credentials are configured (*admin* / *admin*), and the host has a new version of iRMC firmware which is at least 7.72F.

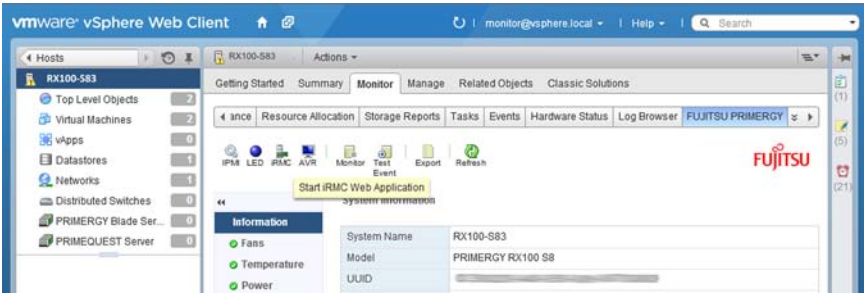


Figure 10: Example: vCenter user "monitor" and iRMC access with SSO as iRMC user "user" - vSphere Web Client

SV Plug-in:

The figure 11 shows the iRMC Web Interface as logged in as user *admin*, but has LAN channel privilege *user*. The user *admin* can only perform actions which are allowed for a user (for example *Toggle location button LED*) but cannot perform system shutdowns or configure the system in any way.

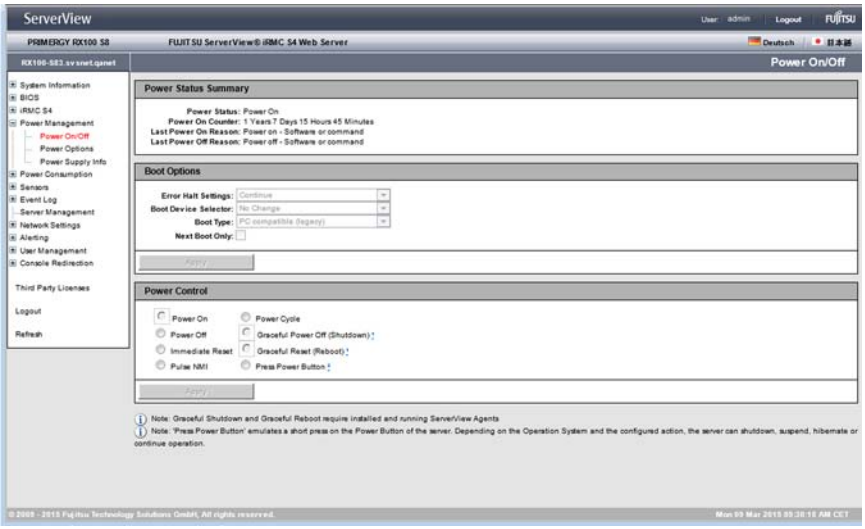


Figure 11: Example: vCenter user "monitor" and iRMC access with SSO as iRMC user "user" - SV Plug-in

5.3.4.3 vCenter user "monitor2" and iRMC "user" access and extended privilege "RemoteStorage"

Situation:

In this example, the vCenter administrator will create a user *monitor2*. This user should start iRMC S4 with SSO as iRMC user *user* but also be able to mount a remote image.

In this case it is necessary to grant the role more privileges than are predefined.

If you need to change the privileges in one of the FUJITSU PRIMERGY role definitions, clone the role and change the privileges in the clone.

If you update the SV Plug-in version, or connect the vCenter to another SVvCenter Service, the role definitions will be overwritten!

The vCenter administrator has to perform the following:

- Updating the firmware of the iRMC S4 to at least version 7.73F.
- Configuring IPMI credentials with a user account who has LAN channel privilege *administrator* or *OEM*.
- In the object navigator of the vSphere Web Client under *Administration* - *Roles*:
  - Choosing the *FUJITSU PRIMERGY Plug-in Monitor* role and cloning this role.
  - Renaming this clone *PluginMonitorPlusStorage*.
  - Adding the privilege *Host->Configuration->Storage Partition Configuratio*n to the *FUJITSU PRIMERGY Plug-in Monitor* role.
  - Saving the *FUJITSU PRIMERGY Plug-in Monitor* role.
- Creating a new vCenter user named *monitor2*.
- Navigating to the vCenter or host for which the user should have this functionality:
  - Selecting *All vCenterActions* - *Add Permission in the context menu*.
  - Selecting the user *monitor2* and assigning the role *PluginMonitorPlusStorage*.

vSphere Web Client:

Logged in as *monitor2*, the user can navigate to the SV Plug-in view for the host and start the iRMC Web Interface:

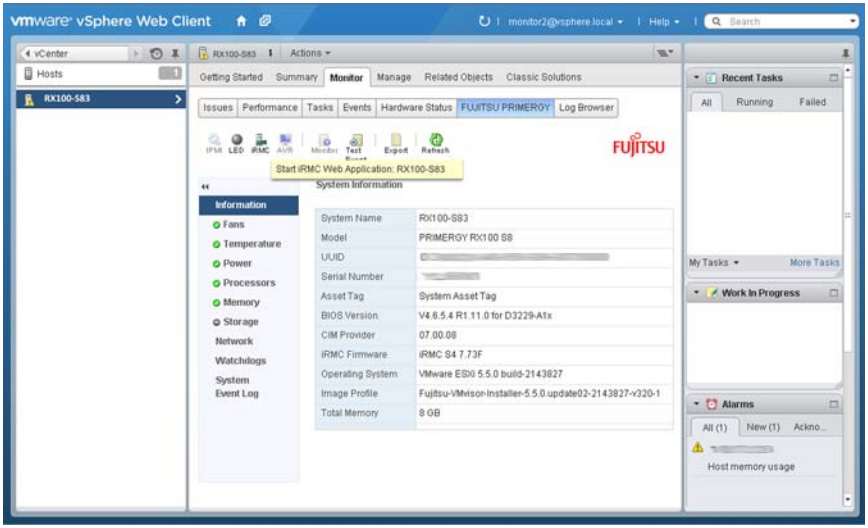


Figure 12: Example: vCenter user "monitor2" and iRMC "user" access and extended privilege "RemoteStorage" - vSphere Web Client

SV Plug-in:

Logged in as the iRMC administrator *admin*, but only with the LAN channel privilege of *user* - but the user can additionally perform remote storage actions:

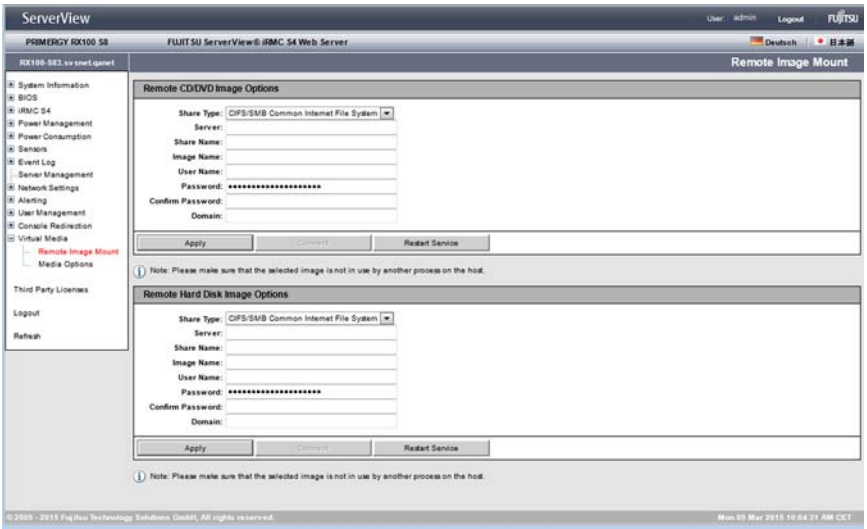


Figure 13: Example: vCenter user "monitor2" and iRMC "user" access and extended privilege "RemoteStorage" - SV Plug-in

6 SV Plug-in Getting Started and Summary

The SV Plug-in offers you a home page with a *Getting Started* tab and a *Summary* tab, which gives an overview of the information items provided by the SV Plug-in. Additionally, there is a *Manage* tab, which lists all FUJITSU PRIMERGY events, shows the FUJITSU PRIMERGY alarms and the role definitions which can be used to assign permissions to an entity (see "FUJITSU PRIMERGY vCenter role definitions and iRMC single sign-on" on page 42).

6.1 Entry point

In the *Home* page of the vSphere Web Client you find two links:

– In the object navigator of the vSphere Web Client the link *FUJITSU PRIMERGY*.

– In the main workspace of the vSphere Web Client the link *FUJITSU ServerView Suite*.

Both links lead to the *Getting Started* tab of the home page of the SV Plug-in.

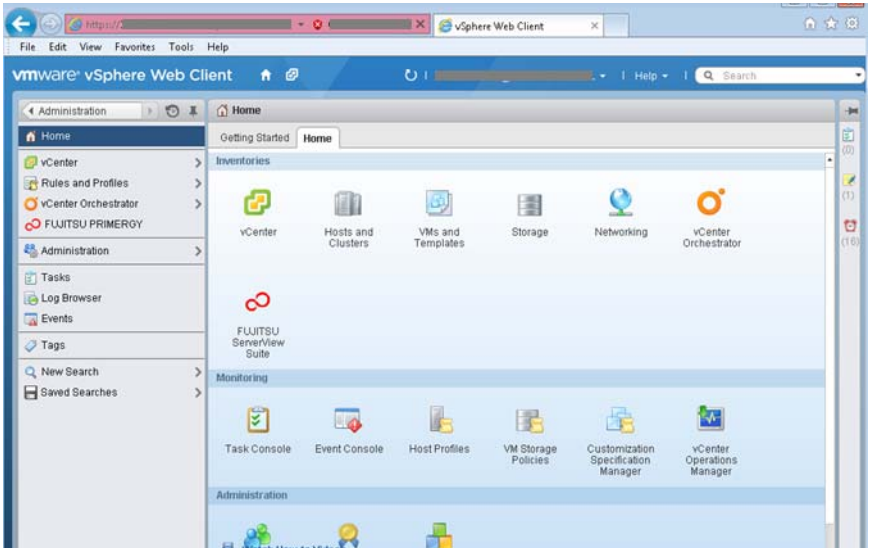


Figure 14: Links to the Getting Started tab of the home page of the SV Plug-in

6.2 Tabs of the home page of the SV Plug-in

The home page of the SV Plug-in has the following tabs:

Getting Started
: The *Getting Started* tab of the home page of the SV Plug-in gives general information about the SV Plug-in (see "Tab Getting Started" on page 58).

Summary
: The *Summary* tab of the home page gives an overview of the information items provided by the SV Plug-in (see "Tab Summary" on page 59).

Manage
: The *Manage* tab of the home page of the SV Plug-in offers three sub-tabs: *Event Definitions*, *Alarm Definitions* and *Role Definitions*.

  The sub-tab *Event Definitions* of the *Manage* tab of the home page of the SV Plug-in lists the event definitions with are set by the SV Plug-in (see "Event Definitions" on page 61).

  The sub-tab *Alarm Definitions* of the *Manage* tab of the home page of the SV Plug-in lists the predefined FUJITSU PRIMERGY alarms (see "Alarm Definitions" on page 62).

  The sub-tab *Role Definitions* of the *Manage* tab of the home page of the SV Plug-in lists the role definitions which can be used to assign permissions to an entity (see "Role Definitions" on page 63 and "FUJITSU PRIMERGY vCenter role definitions and iRMC single sign-on" on page 42).

6.3 Tab Getting Started

The *Getting Started* tab of the home page of the SV Plug-in gives general information about the SV Plug-in.

At the bottom of the getting-started page of the SV Plug-in you find amongst others the following links:

Manage the SVvCenter Services
: Links to the *SVvCenter Service Configuration Overview* view (see "Integration in the event management of the vSphere Web Client" on page 107 and "SVvCenter Service configuration" on page 37).

ServerView Plug-in Manual

Links to the online version of the user guide *ServerView Plug-in for VMware vCenter*.

6.4 Tab Summary

The *Summary* tab of the home page gives an overview of the information items provided by the SV Plug-in:

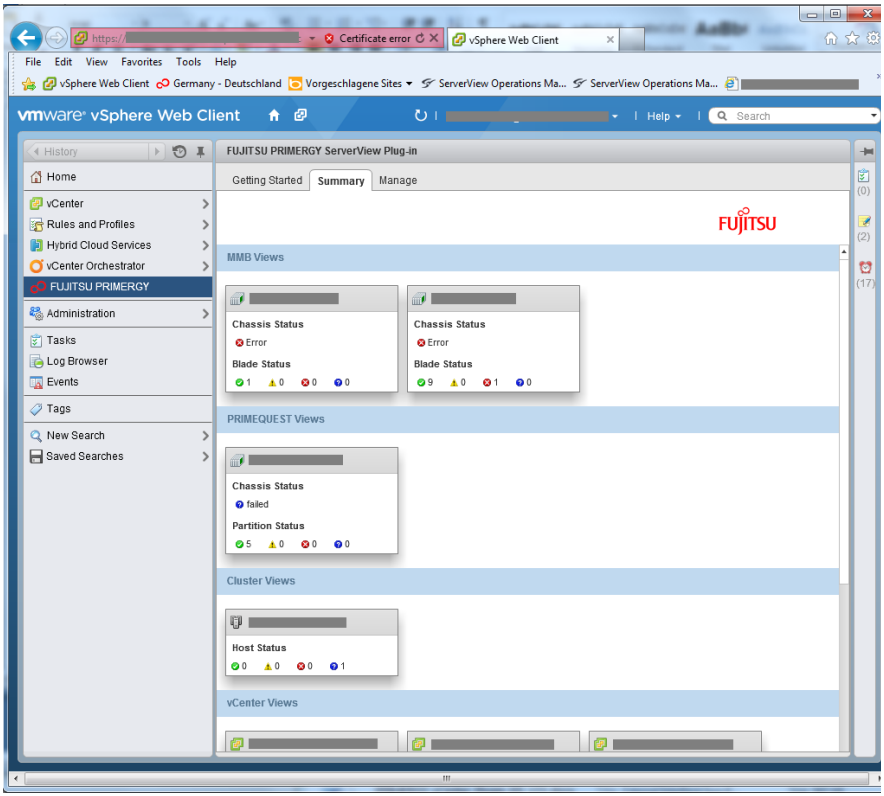


Figure 15: Summary tab of the home page of the SV Plug-in

MMB Views

An overview of all PRIMERGY blade servers discovered by the SVvCenter Service. Additionally, you can see the status of the hosts of the PRIMERGY blade servers.

- ► Click the title of an item box to open the view with detailed information about this MMB node (see "SV Plug-in information of an MMB node" on page 83).

PRIMEQUEST Views

An overview of all PRIMEQUEST systems discovered by the SVvCenter Service. Additionally, you can see the status of the partitions of the PRIMEQUEST systems.

- ► Click the title of an item box to open the view with detailed information about this PRIMEQUEST system (see "SV Plug-in information of a PRIMEQUEST system" on page 93).

Cluster Views

An overview of all clusters discovered by the SVvCenter Service. Additionally, you can see the status of the hosts of the clusters.

- ► Click the title of an item box to open the view with detailed information about this cluster (see "Monitoring vCenter or cluster host servers" on page 101).

vCenter Views

An overview of all vCenters discovered by the SVvCenter Service. Additionally, you can see the status of the hosts of the vCenters.

- ► Click the title of an item box to open the view with detailed information about this vCenter (see "Monitoring vCenter or cluster host servers" on page 101).

SVvCenter Services

An overview of all SVvCenter Services that are available. Additionally, you can see the status of the hosts of the SVvCenter Services.

- ► Click the title of an item box to open the view with detailed information about this SVvCenter Service (see "Properties of SVvCenter Services" on page 111).

6.5 Tab Manage

The *Manage* tab of the home page of the SV Plug-in offers two sub-tabs: *Event Definitions* and *Alarm Definitions*.

6.5.1 Event Definitions

The sub-tab *Event Definitions* of the *Manage* tab of the home page of the SV Plug-in lists the event definitions which are set by the SV Plug-in. If you have more than one vCenter in your environment, you can choose under *Providers* for which vCenter you would like to view the definitions.

If the hosts are monitored by the SVvCenter Service, these indications will be forwarded to the vCenter event management (see "Integration in the event management of the vSphere Web Client" on page 107). The SVvCenter Service listens also to SNMP traps send by registered MMBs (see "SVvCenter Service for MMBs" on page 87) and PRIMEQUEST systems (see "SVvCenter Service for PRIMEQUEST systems" on page 98).

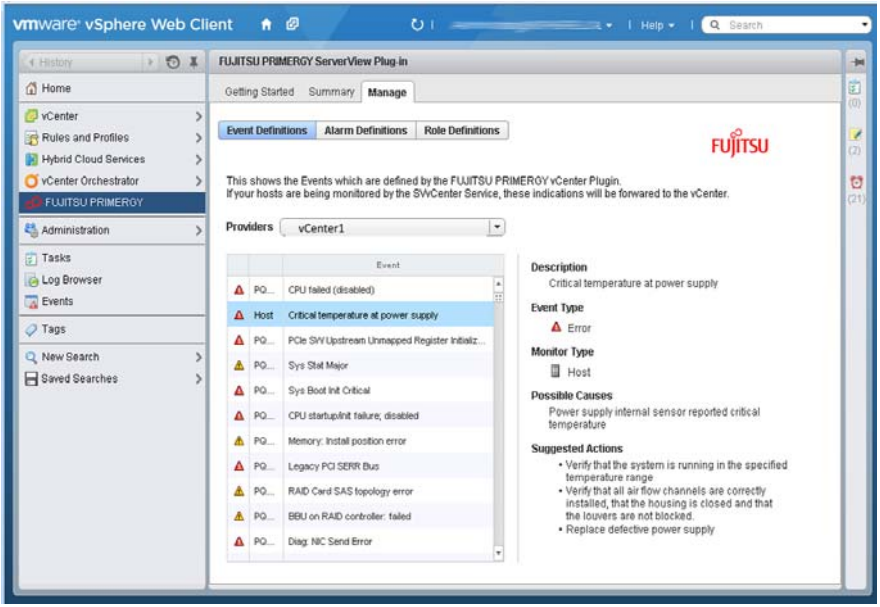


Figure 16: Event Definitions in the Manage tab of the home page of the SV Plug-in

The general list of this tab has the columns *Event Type*, *Monitor Type* and *Description*. You can sort it according to these items.

On the right further information on the selected list entry is displayed.

6.5.2 Alarm Definitions

The sub-tab *Alarm Definitions* of the *Manage* tab of the home page of the SV Plug-in lists the predefined FUJITSU PRIMERGY alarms. If you have more than one vCenter in your environment, you can choose under *Providers* for which vCenter you would like to view the definitions.

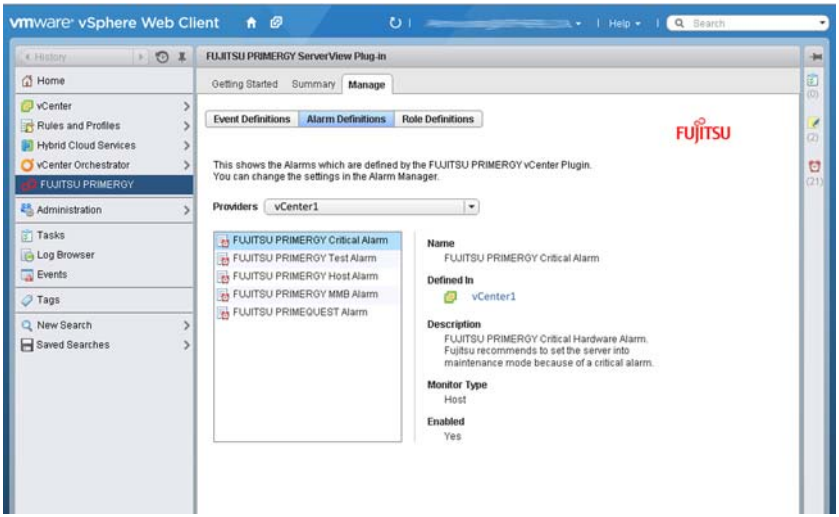


Figure 17: Alarm Definitions in the Manage tab of the home page of the SV Plug-in

The new alarm definitions help you to define specific alarm actions depending on the target type (*Host*, *MMB*, *PRIMEQUEST*) of the event. There is also a test alarm which you can use to test the event/alarm handling in general. This will be triggered from a *test event*. All of these new definitions have no actions and are disabled. To use these you must enable them, and possibly configure an action for each.

The field *Defined In* gives you the name of the vCenter, in which this alarm is defined. This name forms a link to the *Alarm Manager* of this vCenter:

- To open the Alarm Manager of the vCenter, in which an alarm is defined, click the name of the vCenter in the field *Defined In*.

6.5.3 Role Definitions

The sub-tab *Role Definitions* of the *Manage* tab of the home page of the SV Plug-in lists the predefined FUJITSU PRIMERGY roles. If you have more than one vCenter in your environment, you can choose under *Providers* for which vCenter you would like to view the definitions.

This view shows the FUJITSU PRIMERGY vCenter role definitions which are generated during the installation process. They describe the minimum privilege level to perform SV Plug-in actions and can be used to assign permissions to an entity. For further information see "FUJITSU PRIMERGY vCenter role definitions" on page 42.

For further information about the concept and about using these role definitions to limit iRMC functionality, see "FUJITSU PRIMERGY vCenter role definitions and iRMC single sign-on" on page 42.

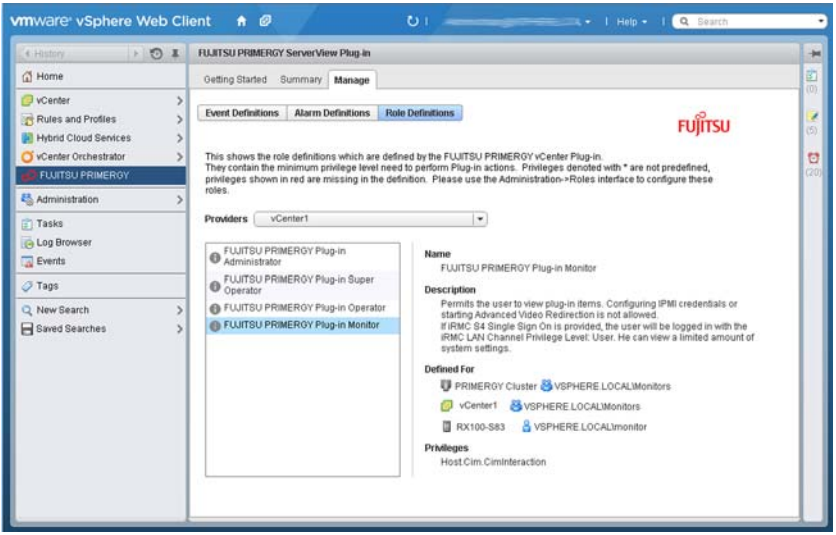


Figure 18: Role Definitions in the Manage tab of the home page of the SV Plug-in

The field *Defined For* gives you the name of the vCenter (Cluster, Host), to which this role definition is assigned. Additional, you can see the user for which the role definition has been assigned.

If the role definitions have been reconfigured after installation, the changes relevant to proper processing of the SV Plug-in will be marked.

*
This privilege was not predefined and has been added after installation. It is not required for proper processing of the SV Plug-in.

*** <in red>
This privilege is been missing. It has been removed since installation and must be added again for proper processing of the SV Plug-in.

7 Monitoring ESXi-based hosts

The SV Plug-in offers extensive possibilities to monitor ESXi-based hosts:

Information on the selected host
: Status icons provide quick and detailed views provide extensive information - see "Information on the selected host - Status items and views" on page 67.

FUJITSU PRIMERGY actions
: A number of action items support calling a monitoring tool or doing settings on the host - see "FUJITSU PRIMERGY Actions (iRMC-based operations)" on page 71.

  If a remote console (AVR) or the iRMC Web Interface is started, the SV Plug-in will consider the privileges of the current user - see "Starting iRMC functions with/without single sign-on" on page 44.

Integration in event management of the vSphere Web Client
: The SV Plug-in includes the *SVvCenter Service* which routes FUJITSU PRIMERGY specific events to the vCenter event management to be monitored in the vSphere Web Client (see "Integration in the event management of the vSphere Web Client" on page 107).

7.1 Access to the SV Plug-in information of an ESXi-based host

- In the object navigator of the vSphere Web Client select *vCenter*.
- Under *Inventory Lists* select *Hosts*.
- Select the desired host.
- Click the *Monitor* tab.

  The *Monitor* tab is displayed, with a set of second-level tabs at the top.

  One of these second level tabs is *FUJITSU PRIMERGY,* which opens the views of the SV Plug-in.

  The *FUJITSU PRIMERGY* second-level tab is only available if two conditions are met:

  – The vendor of the selected host is Fujitsu.

– The version of the ESXi operating system is at least V5.0.

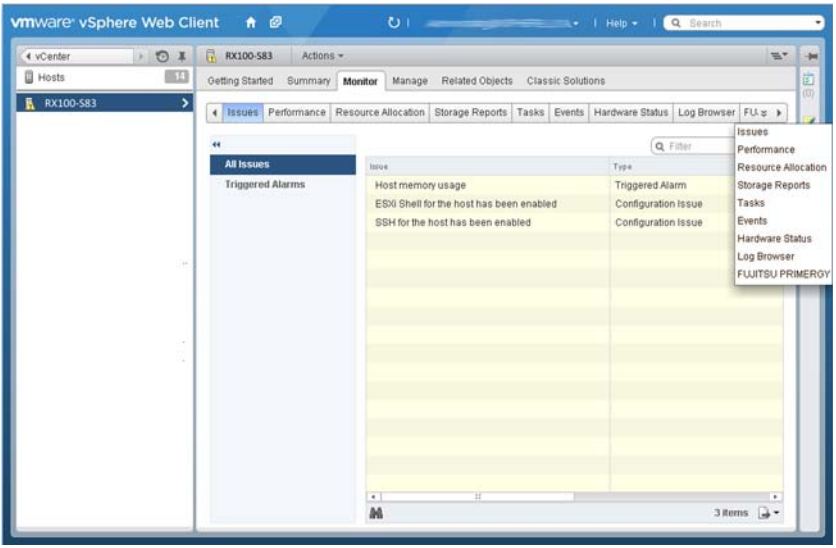


Figure 19: Access to the SV Plug-in information of an ESXi-based host

► Click the *FUJITSU PRIMERGY* subtab to display the interface of the SV Plug-in.

7.2 SV Plug-in information of an ESXi-based host

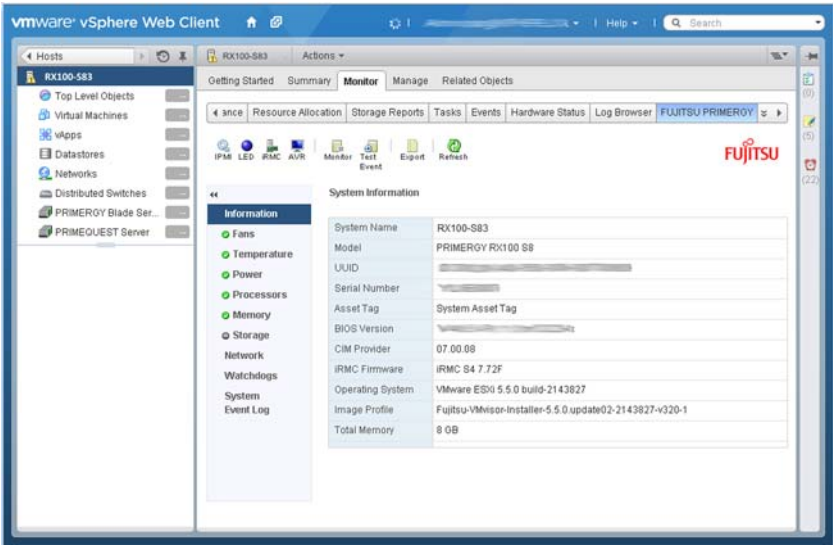


Figure 20: SV Plug-in information of an ESXi host

7.2.1 Information on the selected host - Status items and views

Point in time of data acquisition:

If the SV Plug-in is called, it will retrieve the data of the ServerView CIM providers on the host. Whenever you click the status item tree, the SV Plug-in retrieves the data of the ServerView CIM providers again.

- If you click the *Refresh* icon of vSphere , a new data retrieval cycle will be initiated.

In the main workspace, on the left of the SV Plug-in view, you will find a status item tree:

- Clicking an item provides detailed information to the right of the status item tree.

– In front of the item is a status icon:

ok

degraded

error

not present

If you click this item, no information will be shown to the right of the status item tree.

unknown

retrieving data

– You can collapse or expand the status item tree to allow more/less space for detailed information on the right.

– The detailed information on the right is displayed in tables. You can change the column widths and sort the columns as needed.

Status items and views

With the ServerView ESXi CIM providers V6.31 some new values are available (in the following marked: *SVCIMp*).

For some components the new value *CSS* (customer self service) can be shown. These are components that can be replaced by the customer himself in case of an error.

Information

General information about the host:

System Name, Model, UUID, Serial Number, Asset Tag, BIOS Version, CIM Provider Version, iRMC Firmware Version, Operating System Version, Image Profile, Total Memory

Fans

Information about the fans installed on the system:

Status, Designation, Current Speed, Maximum Speed (SVCIMp< V6.31), Nominal Speed (SVCIMp< V6.31), Fail Reaction, Shutdown Delay, State, Quality (Current Speed / Nominal Speed) (SVCIMp >= V6.31), CSS (SVCIMp >=V6.31)

Information about the fans is not available if you have selected a blade. For information about the fans of a MMB node see "Monitor tab: Information on the selected MMB - Status items and views" on page 84.

Temperature

Detailed information about the temperature sensors installed on the system:

Status, Designation, Temperature, Warning Level, Critical Level, Fail Reaction, State

Power

Information about the power supplies installed in the system:

Status, Designation, State, Product Name (SVCIMp >=V6.31), CSS (SVCIMp >=V6.31)

Information about the power supplies is not available if you selected a blade. For information about the power supplies of a MMB node see "Monitor tab: Information on the selected MMB - Status items and views" on page 84.

Processors

Detailed information about the system processor configuration:

Status, Designation, Frequency (MHz), Manufacturer, Type, L1 Cache, L2 Cache, L3 Cache, Enabled Cores, Cores, Logical Threads, State, CSS (SVCIMp >=V6.31)

Memory

Detailed information about the memory modules installed in the system:

Status, Designation, Type, Size, Frequency (MHz), State, Maximum Frequency (SVCIMp >=V6.31), Voltage (SVCIMp >=V6.31), CSS (SVCIMp >=V6.31), Manufacturer (SVCIMp >=V6.31), Serial Number (SVCIMp >=V6.31)

Storage

Overview of the RAID controllers found and details on their logical drives and physical disks (see "Storage view" on page 76).

Network

Information about the network interfaces configured on the system:

Name, Address Type (primary or iRMC), IP Address, MAC Address

If a component is not accessible, there is no status information available for it.

Watchdogs

Information about the watchdogs configured on the system:

Type, Active, Action, Timeout

If a component is not accessible, there is no status information available for it.

System Event Log

A list of the entries found in the system event log together with cause/resolution information.

The ServerView ESXi CIM providers version 6.31 or later support the System Event Log view. The entries will be retrieved over CIM automatically.

If the ServerView ESXi CIM providers version is less than 6.31, it will be necessary to configure the IPMI credentials (see "IPMI configuration" on page 40) to retrieve the System Event Log entries from the host.

7.2.2 FUJITSU PRIMERGY Actions (iRMC-based operations)

The SV Plug-in offers some *FUJITSU PRIMERGY Actions* depending on the capabilities of the selected host.

To perform the iRMC-based operations (iRMC Web Interface together with single sign-on (SSO), AVR, location button LED and with ServerView ESXi CIM providers version less than 6.31 the System Event Log view), username and password for the IPMI credentials must be configured in the vCenter Server (see "IPMI configuration" on page 40).

These IPMI based actions are always enabled in the context menu, even if the credentials are not configured, or the user does not have the privilege to perform the action. In this case an error message will be shown if the action is started.

7.2.2.1 Starting a FUJITSU PRIMERGY Action

There are two ways to start one of these *FUJITSU PRIMERGY Actions*:

– At the top left of the SV Plug-in interface in the main workspace, up to 8 icons are displayed.

– The *FUJITSU PRIMERGY Actions* can be started independently of the SV Plug-in interface:

  ► In the center pane of the vSphere Web Client select the desired host in the inventory tree.

  ► In the menu *Actions* you will find the submenu *All FUJITSU PRIMERGY Actions*.

  The action *Start MMB Management GUI* is only available as icon at the top left.

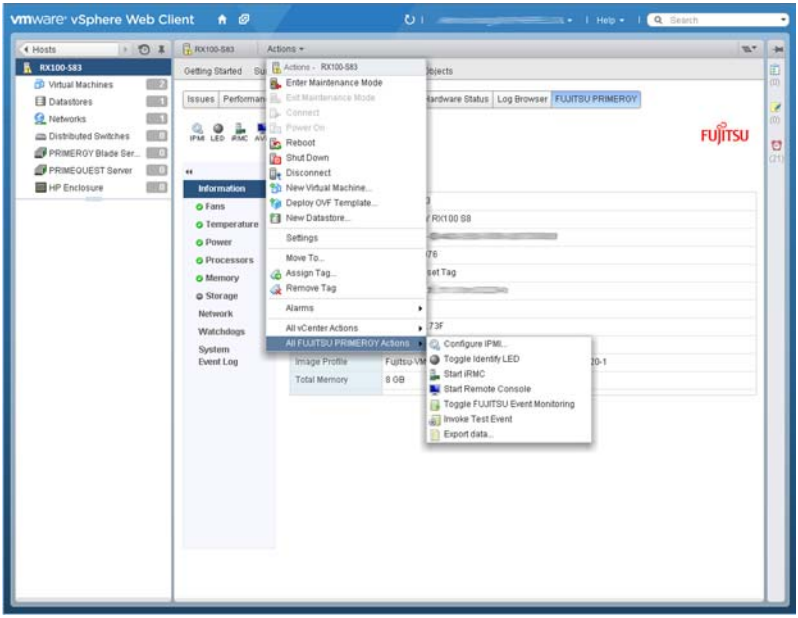


Figure 21: Submenu All FUJITSU PRIMERGY Actions

7.2.2.2 The FUJITSU PRIMERGY Actions

Refresh

► Click this icon to refresh the current view of the SV Plug-in.

This *Refresh* function only refreshes the views/informations of the SV Plug-in - not of the vSphere Web Client.

Consequently, this function is only available among the icons at the top left of the SV Plug-in interface - not in the menu *Actions*.

Configure IPMI ...

► Click this icon to start the IPMI configuration dialog (see "IPMI configuration" on page 40).

Toggle Identify LED

► Click this icon to toggle the Locate LED between on and off:

Locate icon is blue: locate LED is on.

Locate icon is grey: locate LED is off.

The icon is displayed if an iRMC address is available.

Start iRMC

► Click this icon to launch the iRMC Web interface in a new window.

The icon is displayed if an iRMC address is available.

Note "Starting iRMC functions with/without single sign-on" on page 44.

Start Remote Console

► Click this icon to launch a remote console (AVR) in a new window.

The icon is displayed if an iRMC address is available.

Note "Starting iRMC functions with/without single sign-on" on page 44.

Toggle Fujitsu Event Monitoring

► Click this icon to turn off/on the subscription of the host to the SVvCenter Service (see "Integration in the event management of the vSphere Web Client" on page 107).

This action is depicted in four ways, depending on the current status of the subscription:

The host is subscribed to the SVvCenter Service. Events will be monitored by the SVvCenter Service and be forwarded.

The host is not subscribed to the SVvCenter Service. No events will be monitored by the SVvCenter Service and be forwarded.

The subcription status of the host is unknown due to connection problems with the SVvCenter Service. No action will be performed.

The host cannot be subscribed, because the vCenter is not connected to the SVvCenter Service. No action will be performed.

Invoke Test Event

► Click this icon to request the host to send a *Test event* (see "Integration in the event management of the vSphere Web Client" on page 107).

Export Data ...

► Click this icon to open a frame where you can choose data to be exported (host information and System Event Log information).

If you choose all System Event Log entries, the retrieval of data will take some time.

There is a *Cancel* button to leave this frame without action. As long as the export process is running it cannot be stopped and the buttons are locked.

When the requested data has been retrieved, a new window pops up and shows the requested data - with the option to save it to a file.

The icon is displayed if an iRMC address is available.

7.3 Storage view

The *Storage* view offers an overview of the RAID controllers found on the host and details on their logical drives and physical disks.

The information on which this view is based comes from the LSI CIM Provider instead of the PRIMERGY CIM Provider which is used for the other views.

The entry for a controller can be expanded to view details about the controller, as well as its logical drives and physical disks:

- Click the arrow in front of a controller entry to get more detailed data.

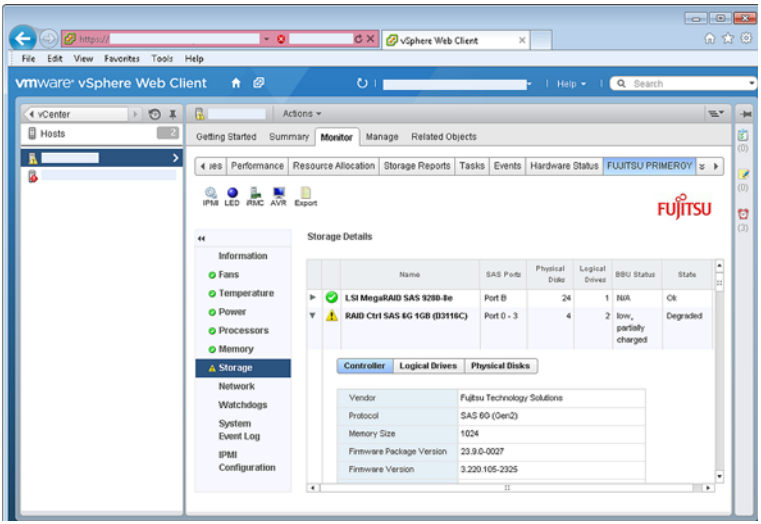


Figure 22: Storage view of the SV Plug-in

Offered Information:

Storage Details

Overview of the RAID controllers found. This information includes:

status of the controller shown as an icon, name of the controller, SAS ports to which the controller is connected, number of physical disks attached to the controller, number of logical drives configured on the controller, status of the BBU if available, textual status of the controller

Storage Details - expanded controller entry

Information shown here includes:

vendor, protocol, memory size, firmware package version, firmware version, BIOS version, driver version, patrol read iterations, Vendor/Device ID, Subvendor/Device ID, PCI Bus/Device/Function numbers, number and status of the logical drives (can be expanded), number and status of the physical drives (can be expanded)

Logical Drives - overview

- Click the *Logical Drives* button in a expanded controller entry view (*Storage Details* view).

  An overview on the logical drives of the selected controller is displayed.

The shown information includes:

status of the drive depicted as an icon, name of the drive, RAID level of the drive, logical size of the driven in MB, number of physical disks configured to this drive, textual status of the drive

Logical Drives - details

- Click the arrow in front of a logical drive entry to get more detailed data.

The shown information includes:

stripe size in KB, read mode, write mode, disk cache mode, number and status of the configured physical disks (can be expanded)

Physical Disks - overview

- Click the *Physical Disks* button in a expanded controller entry view (*Storage Details* view).

  An overview on the physical disks of the selected controller is displayed.

The shown information includes:

vendor, model, serial number, firmware version, SAS address, link speed (GB/s), number and status of the logical drives which have configured this disk (can be expanded if more than one logical drive uses this disk)

7.4 System Event Log view

If the ServerView ESXi CIM provider version is less than 6.31, it will be necessary to configure the IPMI credentials (see "IPMI configuration" on page 40) to retrieve the system event log entries from the host.

Prerequisites

ServerView ESXi CIM providers version 6.31 or later are installed on the ESXi-based host

If an iRMC address is available, the ServerView ESXi CIM providers version 6.31 or later supports the System Event Log view. The entries will be retrived over CIM.

ServerView ESXi CIM providers version < 6.31 are installed on the ESXi-based host

If an iRMC address is available and username and password for IPMI configuration are configured in vCenter Server, you can open this *System Event Log* view:

System Event Log view of the SV Plug-in

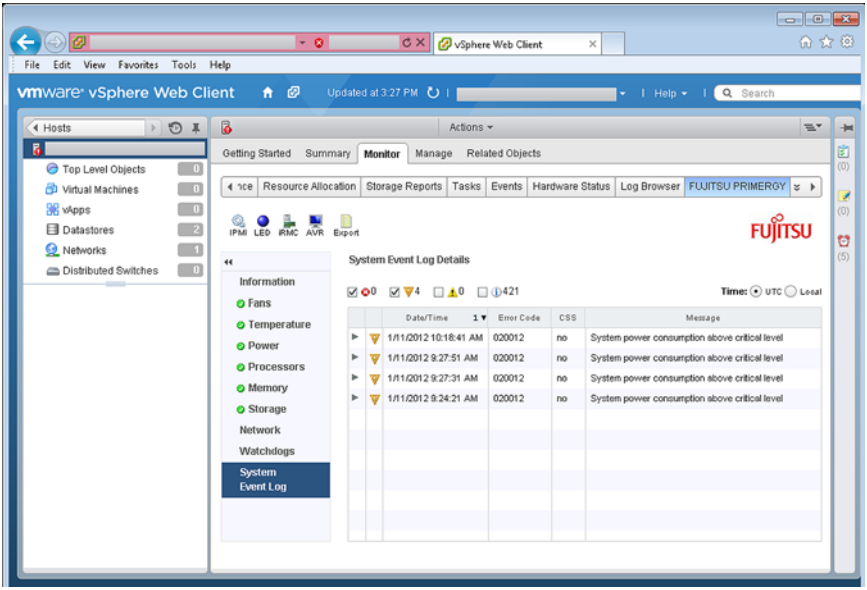
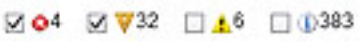


Figure 23: System Event Log view of the SV Plug-in

Choosing quantity and severity of shown entries

A host can have many log entries. Therefore the *System Event Log view* starts only the *Critical* and the *Major* entries showing.

- If you wish to see entries of other severities, check/uncheck the boxes at the top of the *System Event Log Details* list:



Displayed information

For each entry the following information is displayed:

► Click the arrow to get more detailed data.

These details can contain different information: information about the cause of the event as well as helpful information to solve the problem.

Not all messages have these details.

Severity of the entry is displayed as a icon.

Date/Time Date and time either in UTC or local time - depending on the settings seen above the table.

► Change these settings as required.

Error Code Defines the type of the entry.

CSS Shows whether this entry is related to a CSS (Customer Self Service) component.

(Message) Details of the message.

Column sorting

The *System Event Log* table provides for multiple column sorting.

► Click one column header to sort.

Use *Ctrl* and click a second column to sort the table with both columns.

The first column can not be sorted.

8 Monitoring PRIMERGY blade servers

The SV Plug-in adds the new inventory list *PRIMERGY Blade Server* to the object navigator of the vSphere Web Client user interface (see "vSphere Web Client user interface" on page 34).

The following possiblities to monitor a MMB are offered by the SV Plug-in:

– Information about the selected MMB

  Status icons provide quick and detailed views provide extensive information - see "Monitor tab: Information on the selected MMB - Status items and views" on page 84 and "SVvCenter Service for MMBs" on page 87.

– FUJITSU PRIMERGY actions

  A number of actions items support calling a monitoring tool or doing settings on the MMB - see "FUJITSU PRIMERGY Actions" on page 86.

– Integration in event management of the vSphere Web Client

  The SV Plug-in includes the *SVvCenter Service* which routes FUJITSU PRIMERGY specific events to the vCenter event management to be monitored in the vSphere Web Client (see "Integration in the event management of the vSphere Web Client" on page 107).

8.1 Access to the SV Plug-in information of an MMB

The object navigator of the vSphere Web Client shows all MMB nodes, which are related to an ESXi-based host from the set of the assigned vCenter.

The SVvCenter Service (see "SVvCenter Service configuration" on page 37) makes an initial discovery for all MMB.

The SVvCenter Service repeats the discovery procedure on specific events:

– Every time the SVvCenter Service starts

– A new ESXi-based server is added to a vCenter

– An ESXi-based server is removed from a vCenter

– On connection changes (i.e. startup, shutdown)

Procedure:

The SV Plug-in information about the hosts of a vCenter or a cluster is also displayed if you click the title of an item box of a vCenter/cluster in the *Summary* tab of the home page of the SV Plug-in (see "Tab Summary" on page 59).

► In the object navigator of the vSphere Web Client select *vCenter*.

► Under *Inventory Lists* select *PRIMERGY Blade Server*.

A list of all MMB nodes is displayed:

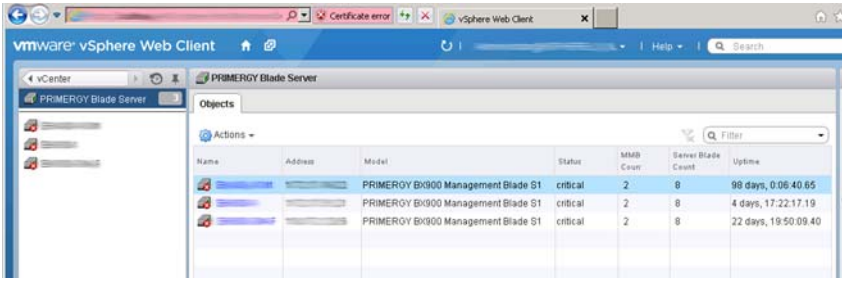


Figure 24: List of all MMB nodes

The list gives general information about each MMB:
system name, IP address, model, status, MMB count, server blade count, uptime

FUJITSU PRIMERGY Actions

Actions

This icon will be displayed if a host is selected in the *Monitor* tab view.

- Click this icon to display the actions context menu (see "FUJITSU PRIMERGY Actions" on page 86).

8.2 SV Plug-in information of an MMB node

- In the MMB node list (see "Access to the SV Plug-in information of an MMB" on page 82) or in the object navigator of the vSphere Web Client select the desired MMB node.

  In the main workspace the information for the selected MMB node is opened, organized in the tabs *Summary*, *Monitor*, and *Related Objects*:

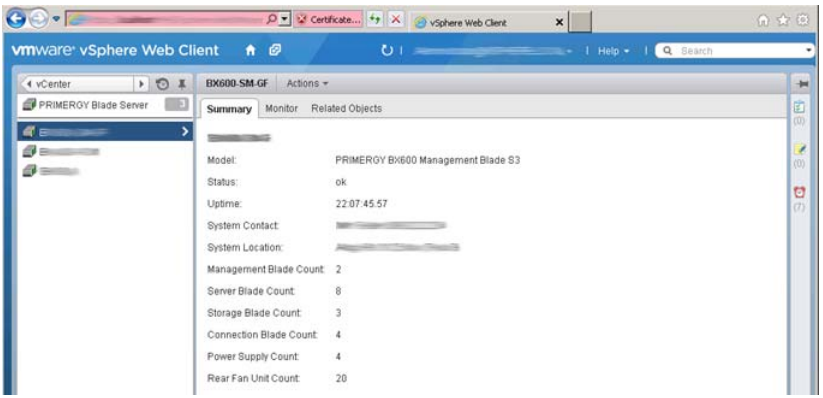


Figure 25: MMB node: Summary tab

There are three tabs with information on the selected MMB node:

Summary

The Summary tab gives general information about the MMB node:

system name, Model, Status, Uptime, System Contact, System Location, Management Blade Count, Server Blade Count, Storage Blade Count, Connection Blade Count, Power Supply Count, Rear Fan Unit Count

Monitor

The *Monitor* tab provides detailed information to the right of the status item tree (see "Monitor tab: Information on the selected MMB - Status items and views" on page 84).

Related Objects

The *Related Objects* tab shows the ESXi hosts which are associated to the selected MMB node.

There is a sub tab in the *Related Objects* tab of a host node showing the inverse relationship.

8.2.1 Monitor tab: Information on the selected MMB - Status items and views

Point in time of data acquisition:

The data is retrieved from the SNMP agent of the MMB every time you select an item in the status tree.

- ► If you click the *Refresh* icon of vSphere , a new data retrieval cycle will be initiated.

In the main workspace, on the left of the SV Plug-in view, you will find a status item tree:

- ► Clicking an item provides detailed information to the right of the status item tree.
- – In front of the item is a status icon:

ok

warning

- critical
- unknown
- retrieving data

– You can collapse or expand the status item tree to allow more/less space for detailed information on the right.

– The detailed information on the right is displayed in tables. You can change the column widths and sort the columns as needed.

– FUJITSU PRIMERGY Actions

Actions

This icon will be displayed if a host is selected in the *Monitor* tab view.

► Click this icon to display the actions context menu (see "FUJITSU PRIMERGY Actions" on page 86).

Status items and views

Information

General information about the MMB node:

System Name, Model, Management Address, Serial Number, Firmware Version, Asset Tag, Rack Name, Managed by VIOM, Status of the Identify LED

Fans

Information about the fans installed in the chassis:

Status, Designation, Current Speed, Maximum Speed, Nominal Speed, Fail Reaction, State

Temperature

Detailed information about the temperature sensors installed in the chassis:

Status, Destination, Temperature, Warning Level, Critical Level, Fail Reaction, State

Power

Information about the power supplies installed in the chassis:

Status, Designation, State

Management Blades

Detailed information about the installed management blades:

Status, Name with Slot ID, Role, Model, Serial Number, Asset Tag

Server Blades

Detailed information about the installed server blades:

Status, Name with Slot ID, Host Name, Model, Serial Number, Asset Tag, Status of the Identify LED, Textual Status

If the MMB hosts an ESXi-based host the *Host Name* is displayed as a hyperlink. You can directly switch to the host view by clicking the link.

Storage Blades

Detailed information about the installed storage blades:

Status, Name with Slot ID, Model, Serial Number, Asset Tag, Status of the Identify LED, Textual Status

Connection Blades

Detailed information about the installed connection blades:

Status, Name with Slot ID, Model, Firmware Number, Serial Number, Asset Tag, Status of the Identify LED, Textual Status

8.2.2 FUJITSU PRIMERGY Actions

The SV Plug-in offers some *FUJITSU PRIMERGY Actions*.

At the top left of the SV Plug-in interface, up to 3 icons are displayed:

For security reasons, a test trap from a MMB can only be triggered on the remote management page of a MMB.

Refresh

► Click this icon to refresh the current view of the SV Plug-in.

This *Refresh* function only refreshes the views/informations of the SV Plug-in - not of the vSphere Web Client.

Consequently, this function is only available among the icons at the top left of the SV Plug-in interface - not in the menu *Actions*.

Configure SNMP ...

► Click this icon to start the SNMP community configuration dialog. Here you can set the community for the selected MMB (see "SNMP settings" on page 88).

Start MMB GUI

► Click this icon to launch the MMB GUI in a new window.

8.3 SVvCenter Service for MMBs

If a PRIMERGY CPU blade is found as a host on a connected vCenter, the SVvCenter Service performs a discovery for blade servers. The SVvCenter Service listens to SNMP traps sent by registered MMBs.

8.3.1 Overview

The SVvCenter Service performs an initial discovery for MMBs. It repeats this discovering procedure on special events.

The SVvCenter Service performs the following steps for all hosts of its vCenter list:

– Check if a host is a server blade

– Retrieves information about the associated hosts (i.e. IP address)

– Stores information about the relationship in an internal database
– Stores additional information about the MMB in an internal database (i.e. instance, system name, model, IP address, SNMP community)

It performs this procedure on special events:

ServerView ESXi CIM providers have to be installed on the ESXi-based host.

– Every time the SVvCenter Service starts
– If a new ESXi-based host is added to a vCenter
– If an ESXi-based host is removed from a vCenter
– On connection changes (i.e. startup, shutdown)

8.3.2 SNMP settings

To use the blade server support of the SV Plug-in the following prerequisites have to be fulfilled:

In the SVvCenter Service Configuration Overview:
Specify the default SNMP communities to be used when a new MMB is detected by the SVvCenter Service, see "Opening the SVvCenter Configuration Overview" on page 110.

In the MMB view:
Set the community for the selected MMB, see "FUJITSU PRIMERGY Actions" on page 86. For example, when the value has changed for the MMB.

The SVvCenter Service also listens to SNMP traps send by registered MMBs. To use this feature you need to make sure that the SVvCenter Service is configured as a trap destination.

8.3.3 Receiving SNMP traps

The SVvCenter Service listens to SNMP traps sent by registered MMBs.

SVvCenter Service has to be configured as a trap destination on the registered MMBs.

In contrast to CIM indications a SNMP trap is processed for all ESXi-based hosts associated to the sending MMB. Therefore, you find the SNMP trap in the event management and logs of the vCenter that hosts the ESXi-based node. If a MMB has multiple hosts in the same vCenter, you will find the event repeatedly.

Only SNMP traps with a serverity *major* or *critical* and the test trap are to be processed.

For security reasons, a test trap from an MMB can only be triggered on the remote management page of an MMB.

9 Monitoring PRIMEQUEST systems

The SV Plug-in adds the new inventory list *PRIMEQUEST Server* to the object navigator of the vSphere Web Client user interface (see "vSphere Web Client user interface" on page 34).

The following possiblities to monitor a PRIMEQUEST system are offered by the SV Plug-in:

– Information about the selected PRIMEQUEST system

  Status icons provide quick and detailed views provide extensive information - see "Monitor tab: Information on the selected PRIMEQUEST system - Status items and views" on page 94 and "SVvCenter Service for PRIMEQUEST systems" on page 98.

– FUJITSU PRIMERGY actions

  A number of actions items support calling a monitoring tool or doing settings for the PRIMEQUEST systems - see "FUJITSU PRIMERGY Actions" on page 97.

– Integration in event management of the vSphere Web Client

  The SV Plug-in includes the *SVvCenter Service* which routes FUJITSU PRIMERGY specific events to the vCenter event management to be monitored in the vSphere Web Client (see "Integration in the event management of the vSphere Web Client" on page 107).

9.1 Access to the SV Plug-in information of a PRIMEQUEST system

The object navigator of the vSphere Web Client shows all PRIMEQUEST systems, which are related to an ESXi-based host from the set of the assigned vCenter.

The SVvCenter Service (see "SVvCenter Service configuration" on page 37) makes an initial discovery for all PRIMEQUEST systems.

The SVvCenter Service repeats the discovery procedure on specific events:

– Every time the SVvCenter Service starts

– A new ESXi-based server is added to a vCenter

– An ESXi-based server is removed from a vCenter

– On connection changes (i.e. startup, shutdown)

Procedure:

The SV Plug-in information about the hosts of a vCenter or a cluster is also displayed if you click the title of an item box of a vCenter/cluster in the *Summary* tab of the home page of the SV Plug-in (see "Tab Summary" on page 59).

► In the object navigator of the vSphere Web Client select *vCenter*.

► Under *Inventory Lists* select *PRIMEQUEST Server*.

A list of all PRIMEQUEST systems is displayed:

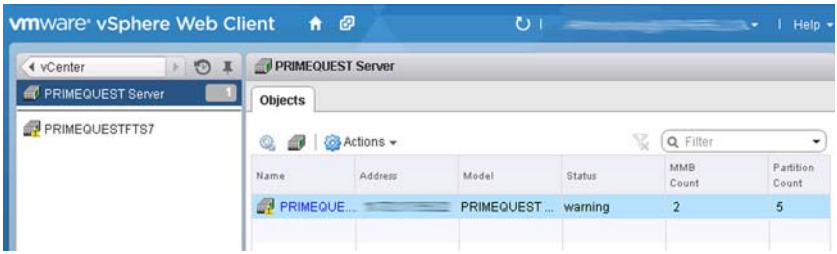


Figure 26: List of all PRIMEQUEST systems

The list gives general information about each PRIMEQUEST system:

system name, IP address, model, status, MMB count, partition count, uptime

FUJITSU PRIMERGY Actions

Actions

This icon will be displayed if a host is selected in the *Monitor* tab view.

- Click this icon to display the actions context menu (see "FUJITSU PRIMERGY Actions" on page 97).

9.2 SV Plug-in information of a PRIMEQUEST system

- In the *PRIMEQUST Server* list (see "Access to the SV Plug-in information of a PRIMEQUEST system" on page 92) or in the object navigator of the vSphere Web Client select the desired PRIMEQUEST system.

  In the main workspace the information for the selected PRIMEQUEST system is opened, organized in the tabs *Summary*, *Monitor*, and *Related Objects*:

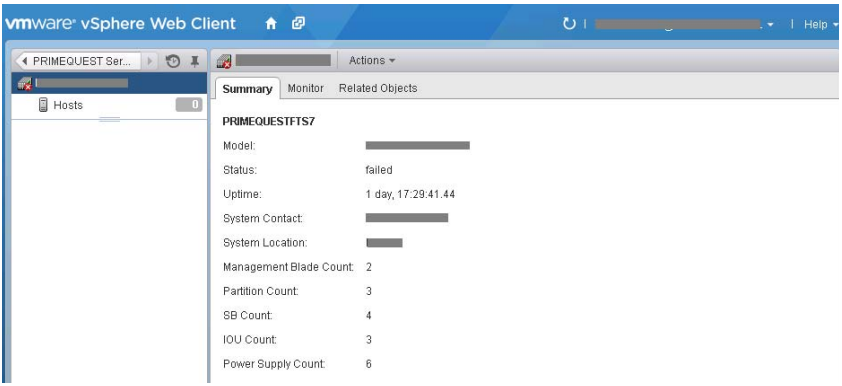


Figure 27: PRIMEQUEST system: Summary tab

There are three tabs with information on the selected PRIMEQUEST system:

Summary

The Summary tab gives general information about the PRIMEQUEST system:

System Name, Model, Status, Uptime, System Contact, System Location, Management Blade Count, Partition Count, System Board (SB) Count, IO Unit (IOU) Count, Power Supply Count

Monitor

The *Monitor* tab provides detailed information to the right of the status item tree (see "Monitor tab: Information on the selected PRIMEQUEST system - Status items and views" on page 94).

Related Objects

The *Related Objects* tab shows the ESXi hosts which are associated to the selected PRIMEQUEST node.

There is a sub tab in the *Related Objects* tab of a host node showing the inverse relationship.

9.2.1 Monitor tab: Information on the selected PRIMEQUEST system - Status items and views

Point in time of data acquisition:

The data is retrieved from the SNMP agent of the PRIEMQUEST system every time you select an item in the status tree.

- ► If you click the *Refresh* icon of vSphere , a new data retrieval cycle will be initiated.

In the main workspace, on the left of the SV Plug-in view, you will find a status item tree:

- ► Clicking an item provides detailed information to the right of the status item tree.
- – In front of the item is a status icon:

ok

warning

- critical
- unknown
- retrieving data

– You can collapse or expand the status item tree to allow more/less space for detailed information on the right.

– The detailed information on the right is displayed in tables. You can change the column widths and sort the columns as needed.

– FUJITSU PRIMERGY Actions

Actions

This icon will be displayed if a host is selected in the *Monitor* tab view.

► Click this icon to display the actions context menu (see "FUJITSU PRIMERGY Actions" on page 97).

Status items and views

Information

General information about the PRIMEQUEST system:

System Name, Model, Management Address, Serial Number, Firmware Version

Fans

Information about the fans installed in the chassis:

Status, Designation, Speed (RPM), Fail Reaction, State

Temperature

Detailed information about the temperature sensors installed in the chassis:

Status, Designation, Temperature, Warning Level, Critical Level, Fail Reaction, State

Power

Information about the power supplies installed in the chassis:

Status, Designation, State

Management Blades

Detailed information about the installed management blades:

Status, Name, Serial Number, Asset Tag

Partitions

Detailed information about the system partitions:

Status, Name, Current Boot State, Asset Tag, State

SB Details

Detailed information about the installed system boards:

Status, Name, Serial Number, Asset Tag, State

IOU Details

Detailed information about the installed I/O units:

Status, Name, Serial Number, Asset Tag, State

DU Details

Detailed information about the installed disk units:

Status, Name, Serial Number, Asset Tag, State

PciBoxes

Detailed information about the installed PRIMEQUEST PCI boxes:

Status, Name, Serial Number, Asset Tag, State

Processors

Detailed information about the system processor configuration:

Status, Designation, Type, L3 Cache (KB), State

Memory

Detailed information about the memory modules installed in the system:

Status, Designation, Size (MB), State

Voltages

Detailed information about the voltage sensors within the system:

Status, Designation, Current Value, Minimum Level, Maximum Level, State

9.2.2 FUJITSU PRIMERGY Actions

The SV Plug-in offers some *FUJITSU PRIMERGY Actions*.

At the top left of the SV Plug-in interface, up to 3 icons are displayed:

Refresh

► Click this icon to refresh the current view of the SV Plug-in.

This *Refresh* function only refreshes the views/informations of the SV Plug-in - not of the vSphere Web Client.

Consequently, this function is only available among the icons at the top left of the SV Plug-in interface - not in the menu *Actions*.

Configure SNMP ...

► Click this icon to start the SNMP community configuration dialog. Here you can set the community for the selected MMB (see "SNMP settings" on page 99).

Start MMB GUI

► Click this icon to launch the *PRIMEQUEST Management Board WEB UI* in a new window.

9.3 SVvCenter Service for PRIMEQUEST systems

The SVvCenter Service performs a discovery for PRIMEQUEST systems. The service checks for each ESXi host on the connected vCenters whether the host is a PRIMEQUEST partition. In case of a partition the SVvCenter Service adds the associated PRIMEQUEST to the inventory list and listen to SNMP traps sent from the discovered PRIMEQUEST systems.

9.3.1 Overview

The SVvCenter Service performs an initial discovery for PRIMEQUEST systems and repeats a discovering procedure on special events.

On startup the SVvCenter Service performs the following steps for all hosts of its vCenter list:

– Check if a host is a partition or a PRIMEQUEST system

– Retrieves information about the associated PRIMEQUEST (i.e. IP address)

– Stores information about the relationship in an internal database

– Stores additional information about the PRIMEQUEST system in an internal database (i.e. instance, system name, model, IP address, SNMP community)

It performs this procedure on special events:

ServerView ESXi CIM providers have to be installed on the ESXi-based host.

– Every time the SVvCenter Service starts

– If a new ESXi-based host is added to a vCenter

– If an ESXi-based host is removed from a vCenter

– On connection changes (i.e. startup, shutdown)

9.3.2 SNMP settings

To use the PRIMEQUEST system support of the SV Plug-in the following prerequisites have to be fulfilled:

In the SVvCenter Service Configuration Overview:

- Specify the default SNMP communities to be used when a new PRIMEQUEST system is detected by the SVvCenter Service, see "Opening the SVvCenter Configuration Overview" on page 110.

In the PRIMEQUEST view:

- Set the community for the selected PRIMEQUEST system, see "FUJITSU PRIMERGY Actions" on page 97. For example, when the value has changed for the PRIMEQUEST system.
- The community must be registered on the PRIMEQUEST Management Board WEB UI for the SVvCenter Service and the vSphere Web Client.

  You will find this setting on the PRIMEQUEST Management Board WEB UI in the menu:

  Network Configuration - SNMP Configuration - Community

The SVvCenter Service also listens to SNMP traps send by registered PRIMEQUEST systems. To use this feature you need to make sure that the SVvCenter Service is configured as a trap destination.

9.3.3 Receiving SNMP traps

The SVvCenter Service listens to SNMP traps sent by registered PRIMEQUEST systems.

SVvCenter Service has to be configured as a trap destination on the registered PRIMEQUEST systems.

- Configure SVvCenter Service as a trap destination on the registered PRIMEQUEST system.

  You will find this setting on the PRIMEQUEST Management Board WEB UI in the menu:

  Network Configuration - SNMP Configuration - Trap

In contrast to CIM indications a SNMP trap is processed for all ESXi-based hosts associated to the sending PRIMEQUEST system. Therefore, you find the SNMP trap in the event management and logs of the vCenter that hosts the ESXi-based node. If a PRIMEQUEST system has multiple hosts in the same vCenter, you will find the event repeatedly.

Only SNMP traps with a serverity *major* or *critical* and the test trap are to be processed.

For security reasons, a test trap from a PRIMEQUEST system can only be triggered on the remote management page of a PRIMEQUEST system.

10 Monitoring vCenter or cluster host servers

The SV Plug-in offers lists of the hosts assigned to a vCenter or to a cluster.

Via this access point the SV Plug-in offers less information on the single host than via the inventory tree item *Hosts* (see "Monitoring ESXi-based hosts" on page 65), but all FUJITSU PRIMERGY actions are available.

10.1 Access to the SV Plug-in information of the hosts of a vCenter/cluster

The SV Plug-in information about the hosts of a vCenter or a cluster is also displayed if you click the title of an item box of a vCenter/cluster in the *Summary* tab of the home page of the SV Plug-in (see "Tab Summary" on page 59).

- In the object navigator of the vSphere Web Client select *vCenter*.
- Under *Inventory Lists* select *vCenter Servers* or *Clusters*.
- Select the desired vCenter or cluster.
- Click the *Monitor* tab.

  The *Monitor* tab is displayed, with a set of second-level tabs at the top.

  One of these second level tabs is *FUJITSU PRIMERGY,* which opens the views of the SV Plug-in.

  The FUJITSU PRIMERGY second-level tab is only available if two conditions are met:

  – The vendor of the selected host is Fujitsu.

  – The version of the ESXi operating system is at least V5.0.

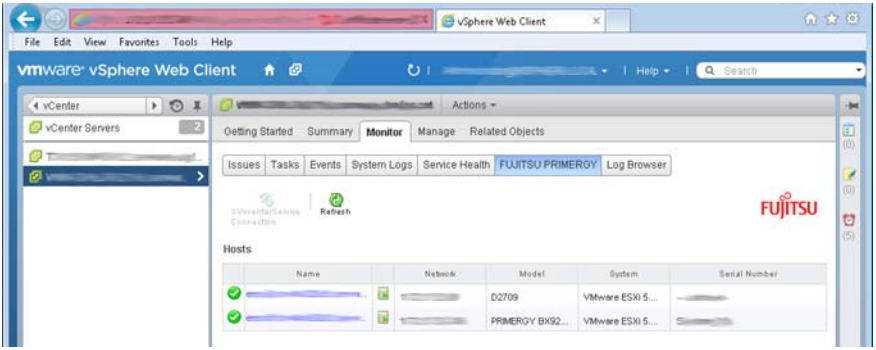


Figure 28: Access to the SV Plug-in information of vCenter servers

► Click the *FUJITSU PRIMERGY* subtab to display the interface of the SV Plug-in.

A list of the hosts found in the vCenter/cluster is shown.

The list gives general information about each host of the vCenter/cluster:

status, host name (with a link to the Single System View for the host, if the host is available), SVvCenter Service monitoring status (subscribed/ not subscribed), network address, model, operating system, serial number

In front of the host name is a status icon:

- ok
- degraded
- error
- not present

  If you click this item, no information will be shown to the right of the status item tree.
- unknown
- retrieving data

10.2 FUJITSU PRIMERGY Actions

Action icons

The SV Plug-in offers some *FUJITSU PRIMERGY Actions* depending on the capabilities of the selected host.

At the top left of the SV Plug-in interface in the main workspace the action icons are displayed.

Point in time of data acquisition:

If the SV Plug-in is called, it will retrieve the data of the ServerView CIM providers on the host. Whenever you click the status item tree, the SV Plug-in retrieves the data of the ServerView CIM providers again.

- If you click the *Refresh* icon of vSphere , a new data retrieval cycle will be initiated.

Refresh

- Click this icon to refresh the current view of the SV Plug-in.

This *Refresh* function only refreshes the views/informations of the SV Plug-in - not of the vSphere Web Client.

Consequently, this function is only available among the icons at the top left of the SV Plug-in interface - not in the menu *Actions*.

SVvCenterService Connection

- Click this icon to start a connection dialog similar to the dialog in the *SVvCenter Service Configuration Overview* (see "SVvCenter Service configuration" on page 37).

If the vCenter is already connected to a SVvCenter Service, you can update the connection or disconnect the vCenter from the SVvCenter Service.

If the vCenter is not connected to a SVvCenter Service, you can connect this vCenter to a selected SVvCenter Service.

Actions

This icon will be displayed if a host is selected in the *Monitor* tab view.

- ► Click this icon to display the actions context menu (see "Actions in the context menu" on page 104).
- ►

Actions in the context menu

(For opening this context menu see "Action icons" on page 103)

Configure IPMI ...

- ► Click this icon to start the IPMI configuration dialog (see "IPMI configuration" on page 40).

Toggle Identify LED

- ► Click this icon to toggle the Locate LED between on and off:

Locate icon is blue: locate LED is on.

Locate icon is grey: locate LED is off.

The icon is displayed if an iRMC address is available.

Start iRMC

- ► Click this icon to launch the iRMC Web interface in a new window.

The icon is displayed if an iRMC address is available.

Note "Starting iRMC functions with/without single sign-on" on page 44.

Start Remote Console

► Click this icon to launch a remote console (AVR) in a new window.

The icon is displayed if an iRMC address is available.

Note "Starting iRMC functions with/without single sign-on" on page 44.

Toggle Fujitsu Event Monitoring

► Click this icon to turn off/on the subscription of the host to the SVvCenter Service (see "Integration in the event management of the vSphere Web Client" on page 107).

This action is depicted in four ways, depending on the current status of the subscription:

The host is subscribed to the SVvCenter Service. Events will be monitored by the SVvCenter Service and be forwarded.

The host is not subscribed to the SVvCenter Service. No events will be monitored by the SVvCenter Service and be forwarded.

The subcription status of the host is unknown due to connection problems with the SVvCenter Service. No action will be performed.

The host cannot be subscribed, because the vCenter is not connected to the SVvCenter Service. No action will be performed.

Invoke Test Event

► Click this icon to request the host to send a *Test trap* (see "Integration in the event management of the vSphere Web Client" on page 107).

Export Data ...

- Click this icon to open a frame where you can choose data to be exported (host information and System Event Log information (iRMC)).

  If you choose all System Event Log entries, the retrieval of data will take some time.

  There is a *Cancel* button to leave this frame without action. As long as the export process is running it cannot be stopped and the buttons are locked.

When the requested data has been retrieved, a new window pops up and shows the requested data - with the option to save it to a file.

The icon is displayed if a iRMC address is available.

Opening the Single System View for a host of a vCenter/cluster

The Single System View will be opend, if a iRMC address is available.

- Click the host name of the desired host in the list (see "Access to the SV Plug-in information of the hosts of a vCenter/cluster" on page 101).

  The Single System View of the desired host is opened.

11 Integration in the event management of the vSphere Web Client

The SV Plug-in includes a *SVvCenter Service* which routes FUJITSU PRIMERGY specific events to the vCenter event management to be monitored in the vSphere Web Client.

If a FUJITSU PRIMERGY host detects a problem, it will create a CIM indication and send it to subscribed destinations. If SVvCenter Service is subscribed to the host, it will receive this CIM indication. It creates a corresponding vCenter event and forwards it to vCenter Server.

Additionally, the SVvCenter Service performs a discovery for blade servers or PRIMEQUEST systems if a PRIMERGY CPU blade or a PRIMEQUEST system is found as a host on a connected vCenter (see "SVvCenter Service Configuration Overview" on page 110). The SVvCenter Service listens to SNMP traps sent by registered MMBs (see "SVvCenter Service for MMBs" on page 87) or registered PRIMEQUEST systems (see "SVvCenter Service for PRIMEQUEST systems" on page 98).

In certain situations some further settings can help you to enhance the performance of the SVvCenter Service for Events, MMBs and PRIMEQUEST systems (see "Further helpful service properties for the SVvCenter Service for Events, MMBs and PRIMEQUEST systems" on page 112).

So the FUJITSU PRIMERGY specific event is shown in the regular *Monitor-Events*-subtab of the vSphere Web Client:

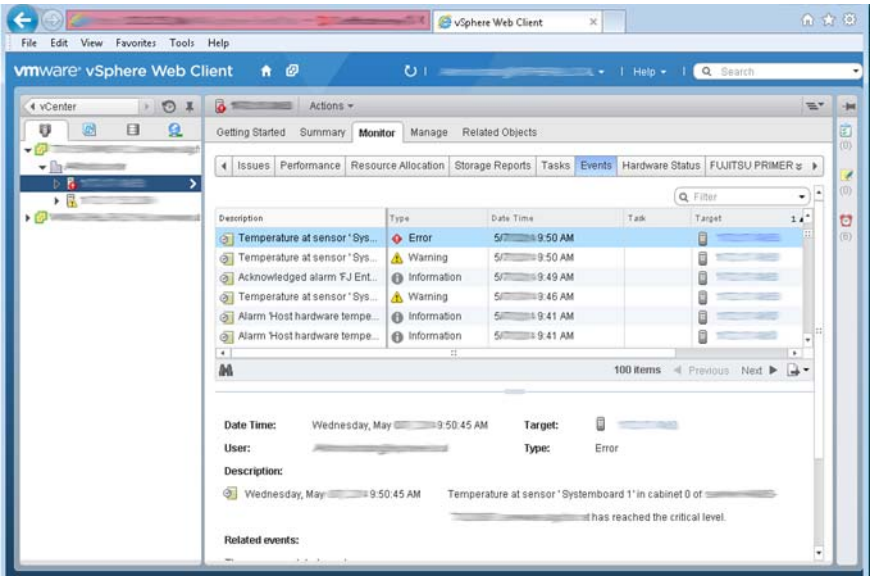

vSphere Web Client
File Edit View Favorites Tools Help
vmware vSphere Web Client
Help
Search
vCenter
Actions
Getting Started Summary Monitor Manage Related Objects
Issues Performance Resource Allocation Storage Reports Tasks Events Hardware Status FUJITSU PRIMER
Filter
Description Type Date Time Task Target
Temperature at sensor 'Sys... Error 9:50 AM
Temperature at sensor 'Sys... Warning 9:50 AM
Acknowledged alarm 'FJ Ent... Information 9:49 AM
Temperature at sensor 'Sys... Warning 9:46 AM
Alarm 'Host hardware tempe... Information 9:41 AM
Alarm 'Host hardware tempe... Information 9:41 AM
100 items
Previous
Next
Date Time: Wednesday, May 9:50:45 AM
Target:
User:
Type: Error
Description:
Wednesday, May 9:50:45 AM
Temperature at sensor 'Systemboard 1' in cabinet 0 of
has reached the critical level.
Related events:

Figure 29: FUJITSU PRIMERGY specific events in the Monitor-Events-subtab of the vSphere Web Client

11.1 Prerequisites

Prerequisites

– CIM and SNMP

  ESXi-based host
  ServerView ESXi CIM providers have to be installed on the ESXi-based host of which events should be displayed in the vSphere Web Client interface.

  MMB
  SVvCenter Service has to be configured as a trap destination on the registered MMBs.

  PRIMEQUEST system
  SVvCenter Service has to be configured as a trap destination on the registered PRIMEQUEST systems.

– SVvCenter Service has to be connected to the vCenter to which the host is assigned to (see "Adding a vCenter to the SVvCenter Service" on page 38).

– The SVvCenter Service must be subscribed to this host (see ”Monitoring vCenter or cluster host servers”: "FUJITSU PRIMERGY Actions" on page 103). You can find an overview of the hosts subcribed to a SVvCenter Service on the *SVvCenter Configuration Overview* (see "SVvCenter Service Configuration Overview" on page 110).

11.2 SVvCenter Service Configuration Overview

You can use this view to manage all of the SVvCenter Services installed in your environment.

11.2.1 Opening the SVvCenter Configuration Overview

At the bottom of the getting-started tab of the home page of the SV Plug-in you find a link *Manage the SVvCenter Services*.

- In the object navigator of the vSphere Web Client select the item *Administration*.
- Select the sub-item *FUJITSU PRIMERGY Administration*.
- Select the sub-item *SVvCenter Service Configuration Overview*.

  In the main workspace of the vSphere Web Client the *SVvCenter Service Configuration Overview* opens:

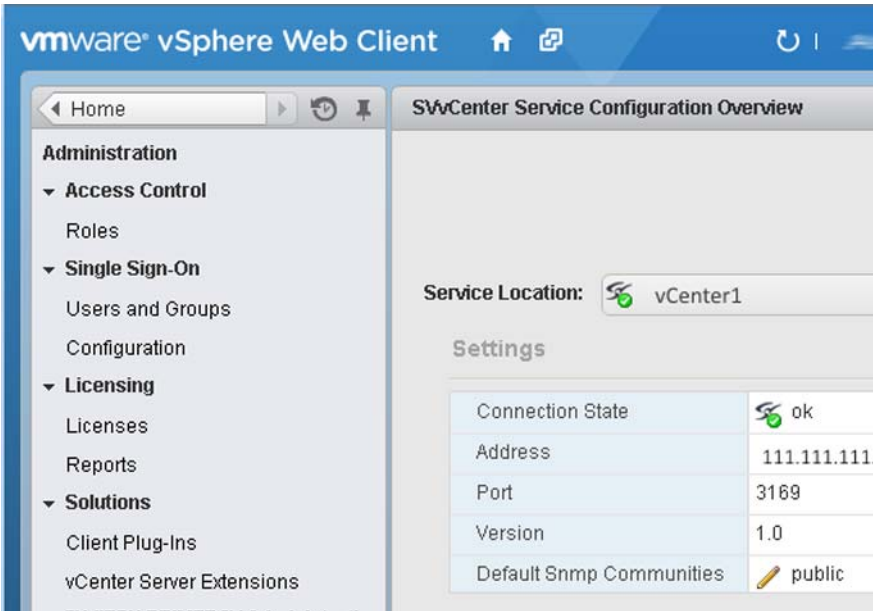


Figure 30: SVvCenter Service Configuration Overview

11.2.2 Properties of SVvCenter Services

The properties of a SVvCenter Service are also displayed if you click the title of an item box of a SVvCenter Service in the *Summary* tab of the home page of the SV Plug-in (see "Tab Summary" on page 59).

- Select one SVvCenter Service in the *Service Location* selection box.

  The current properties of the selected SVvCenter Service are displayed:

Connection State	Current status and connection between the vSphere Web Client and the SVvCenter Service
Address	Address used for the connection
Port	Port used for the connection
Version	Version of the SVvCenter Service
Default Snmp Communities	For discovering blade servers (see "SVvCenter Service for MMBs" on page 87) and PRIMEQUEST systems (see "SVvCenter Service for PRIMEQUEST systems" on page 98). You can edit this list (comma separated) by clicking the pen-icon seen in this area.
vCenter Name	vCenters connected to this SVvCenter Service. The icon before shows the status between the SVvCenter Service and the vCenter. It also shows how many hosts are monitored (subscribed), and how many not.

11.2.3 Further helpful service properties for the SVvCenter Service for Events, MMBs and PRIMEQUEST systems

In certain situations some further settings can help you to enhance the performance of the SVvCenter Service for Events, MMBs and PRIMEQUEST systems.

You can set these properties in the *service.properties* file of the service. It will be found on the system where the service is installed on:

...\Fujitsu\vCenter Integration\service\conf\service.properties

Further service properties

`trap.forward.limit=30`
: Time limit for event forwarding.

  Default value: 30 seconds. Only numeric values.

  Comment: Sometimes events are sent with high intensity. In this case the same event is sent by the same host repeatedly and generates a significant number of entries in the event management of vSphere Web Client. The same event sent by the same host during this time limit won't be forwarded to the vCenter event management.

`cim.client.timeout=3000`
: Timeout value for CIM connections.

  Default value: 3000 milliseconds. Only numeric values.

  Comment: Low connectivity in the network or older versions of CIM providers causes connection timeouts. If you increase this value, there will be a lower number of connection timeouts but the processing time will increase!

`snmp.client.timeout=3000`
: Timeout value for SNMP connections.

  Default value: 3000 milliseconds. Only numeric values.

  Comment: Low connectivity in the network or older versions of SNMP agents causes connection timeouts. If you increase this value, there will be a lower number of connection timeouts but the processing time will increase!

11.2.4 Adding/removing a vCenter to/from the SVvCenter Service

For further information on the following procedures see:

- "Adding a vCenter to the SVvCenter Service" on page 38
- "Updating the vCenter credentials" on page 39
- "Removing a vCenter from the SVvCenter Service" on page 40

11.3 FUJITSU PRIMERGY Predefined Alarm

The SV Plug-in offers a predefined alarm which will be triggered if a warning or error level event has been received by the vSphere Web Client event management. This alarm is enabled but has no actions defined.

You can define a convient action for this predefined alarm in the vSphere Web Client:

Prerequisites:

– Required Privilege: *Alarms.Create Alarm* or *Alarm.Modify Alarm*

Procedure:

- ► In the object navigator of the vSphere Web Client select an inventory object.
- ► Click the *Manage* tab.
- ► Click the sub tab *Alarm Definitions*.
- ► Right-click the list of alarms and select one of the options to add or edit an alarm.

  For further information see the documentation of VMware vSphere.
- ► Click *Finish*.

11.4 Actions related to SVvCenter Service

In the vSphere Web Client views for ESXi-based hosts (see "SV Plug-in information of an ESXi-based host" on page 67 and "FUJITSU PRIMERGY Actions" on page 103) you find the following actions related to the SVvCenter Service:

Toggle Fujitsu Event Monitoring

- Click this icon to turn off/on the subscription of the host to the SVvCenter Service.

  This action is depicted in four ways, depending on the current status of the subscription:

The host is subscribed to the SVvCenter Service. Events will be monitored by the SVvCenter Service and be forwarded.

The host is not subscribed to the SVvCenter Service. No events will be monitored by the SVvCenter Service and be forwarded.

The subcription status of the host is unknown due to connection problems with the SVvCenter Service. No action will be performed.

The host cannot be subscribed, because the vCenter is not connected to the SVvCenter Service. No action will be performed.

Invoke Test Event

- Click this icon to request the host to send a test indication.

  The selected host will be requested to send a test indication to its subscribed nodes.

  If the host is not subscribed to t he SVvCenter Service (see "SVvCenter Service configuration" on page 37), you will not see the event in the vCenter Event Manager (*Monitor-Events*-subtab of the vSphere Web Client).

12 Error handling

12.1 Point in time of data acquisition

If the SV Plug-in is called, it will retrieve the data of the ServerView CIM providers and/or the LSI CIM providers (*Storage* view) on the host. Whenever you click the status item tree (see "Information on the selected host - Status items and views" on page 67), the SV Plug-in retrieves the data of the ServerView CIM providers again.

If you click the *Refresh* icon of vSphere , a new data retrieval cycle will be initiated.

12.2 All expanded items are closed

Once a view with expanded items is refreshed, all expanded items are closed.

- You have to expand the desired items again to see the specific data again.

12.3 Retrieving data failed

If retrieving data fails, an error icon will be displayed at the bottom right of the SV Plug-in interface.

If loading a content view fails, a message box will be displayed showing the possible cause and the original error text.

12.4 An action at the top left of the SV Plug-in interface is disabled

An action at the top left of the SV Plug-in interface will be disabled, if the user doesn't have the required privilege. There will be a tooltip *not privileged to start...* .

See "Starting iRMC functions with/without single sign-on" on page 44.

12.5 An action in the context menu results an error message

The request of an action in the context menu will result an error message, if the user doesn't have the required privilege.

See "Starting iRMC functions with/without single sign-on" on page 44.

12.6 Remote console (AVR) or iRMC Web Client don't work as was to be expected

If the remote console (AVR) or the iRMC Web Client are started from vSphere Web Client, it will be started in the role which matches the current user privileges as previously defined.

If these privileges definitions aren't enough to enable desired functions, AVR and iRMC Web Client will show unexpected behaviour.

See "Starting iRMC functions with/without single sign-on" on page 44.

12.7 The same event generates a significant number of entries in the event management

Sometimes events are sent with high intensity. In this case the same event is sent by the same host repeatedly and generates a significant number of entries in the event management of vSphere Web Client.

The SV Plug-in includes a *SVvCenter Service* which routes FUJITSU PRIMERGY specific events to the vCenter event management to be monitored in the vSphere Web Client.

You can set the `trap.forward.limit` property of this service to enhance its performance.

See "Further helpful service properties for the SVvCenter Service for Events, MMBs and PRIMEQUEST systems" on page 112.

12.8 Repeated connection timeouts

Low connectivity in the network or older versions of CIM providers or SNMP agents causes connection timeouts.

The SV Plug-in includes a *SVvCenter Service* which routes FUJITSU PRIMERGY specific events to the vCenter event management to be monitored in the vSphere Web Client.

You can set the `<cim/snmp>.client.timeout` property of this service to enhance its performance during connection timeouts.

If you increase this value, there will be a lower number of connection timeouts but the processing time will increase!

See "Further helpful service properties for the SVvCenter Service for Events, MMBs and PRIMEQUEST systems" on page 112.